GRIFFIN-CS2 系列使用手冊

思凌科技有限公司

Version 1.3

www.slink.com.tw

思凌科技 GRIFFIN-CS22 系列使用手冊

2006/04/15

版權聲明

簡介

思凌科技 GRIFFIN CHIP SOLUTION VERSION 2（GRIFFIN-CS22）

概述

GRIFFIN-CS2 系列為思凌科技所設計的閘道型企業網路裝置晶片，包含防火牆、Web 伺服器、Mail 伺服器，Mail 病毒防治、Mail 垃圾郵件防治、DNS 伺服器、DHCP 伺服器、FTP 伺服器等常用網路服務功能，其中 Slink 思凌科技所開發的自我偵測機制，能夠自我偵測目前硬體狀況，自動保持網路服務的持續服務，讓企業的網路服務能更加穩定，加上思凌科技所開發的精靈式網路管理介面，使得網路管理更輕鬆自在。GRIFFIN-CS2 系列並提供支援動態網路位置架設，提供企業用撥接線路也能完成網路的建置。

本手冊將以最簡易地、迅速地指導管理者去使用及管理。

主要功能

GRIFFIN-CS2 包含以下主要的網路伺服器功能

- 防火牆（FIREWALL）
- 入侵偵測（IDS）
- 網頁伺服器(APACHE WEB SERVER)
- 郵件伺服器（POSTFIX MAIL SERVER）
- 郵件掃描服務（MAILSCANNER SERVICE）
- 名稱解析伺服器（BIND-9X DNS SERVER）
- 動態網路位置配置伺服器（DHCP SERVER）
- 檔案傳輸服務伺服器（PROFTP FTP SERVER）
- Windows 檔案分享伺服器（SAMBA SERVER）
- 系統自動偵測機制（處理器、記憶體、網路流量及硬碟）
- 交互式伺服器自動回復機制
- CLAMAV 郵件及 Windows 檔案掃毒功能

輔助系統管理功能

GRIFFIN-CS2 系列包含以下主要的系統管理功能

- 系統資訊檢視
- 網路設定精靈
- 使用人員設定及管理（無人數限制）
- 系統備份及還原（支援遠端備份及還原）
- 系統效能教調
- 系統流量監測（處理器、記憶體、及網路流量）
- 郵件報表分析（可以監控即時郵件狀況）

網頁支援功能

GRIFFIN-CS2 系列包含以下主要的網頁支援功能

- PHP 支援
- NAMO 支援
- SSL 網頁加密功能支援
- ZEND OPTIMIZER 支援

GRIFFIN-CS2 系列包含以下主要的網路應用軟體

- WEBMAIL（含 Web DRIVER）

GRIFFIN-CS2 系列可選購下列網路應用程式

- DESKNET'S 企業群組軟體

GRIFFIN-CS2 系列可加裝下列應用程式

- POSTGRESQL
- MYSQL
- SOPHOS 防毒核心

GRIFFIN-CS2 系列可加裝下列自由軟體應用程式

- SLINK PEGAS 網路購物軟體
- MAMBO

附件列表

本產品中應包含下列物品，請先檢視。

- 思凌科技 GRIFFIN-CS2 晶片
- 晶片電源線×1
- 使用手冊光碟×1
- 簡易手冊×1
- 保證書×1

硬體需求

爲了提供最佳的系統需求，GRIFFIN-CS2 要求下列基本產品配備

- X86 機器
- （INTEL、BROADCOM、3COM、REALTEK、DLINK）任一網卡*2
- INTEL 系列 CPU（P3 系列含以上）
- 256MB 以上的記憶體容量
- IDE 或 SCSI 系列硬碟*1（作爲資料硬碟用，如要使用 SCSI 硬碟則需安裝 SCSI 控制卡）
- 一組 IDE 插槽

注意

GRIFFIN-CS2 對於 SCSI 的支援，僅限於一顆 SCSI 硬碟，SCSI 控制卡上請僅安裝一顆 SCSI 硬碟即可，勿安裝其它 SCSI 裝置。

目前 SCSI 及 DEVICE RAID 可以支援的爲下

- ADAPTEC AIC7xxx（含 AIC79xx）系列控制卡
- LSI U160/U320 系列控制卡
- LSI MegaRaid 系列控制卡
- IBM SERVERRAID 5/6

硬體安裝程序

1. 將晶片安裝於 IDE-1 插槽
2. 將新的硬碟接至 IDE-2 或 SATA 插槽（BIOS 需設定爲第二 IDE 裝置或第一 SATA 裝置）
3. 確定機器上安置好 2 片網卡
4. 接上電源線，開啓電源
5. 開始系統安裝管理程序設定
6. 客戶端密碼變更系統的使用

注意

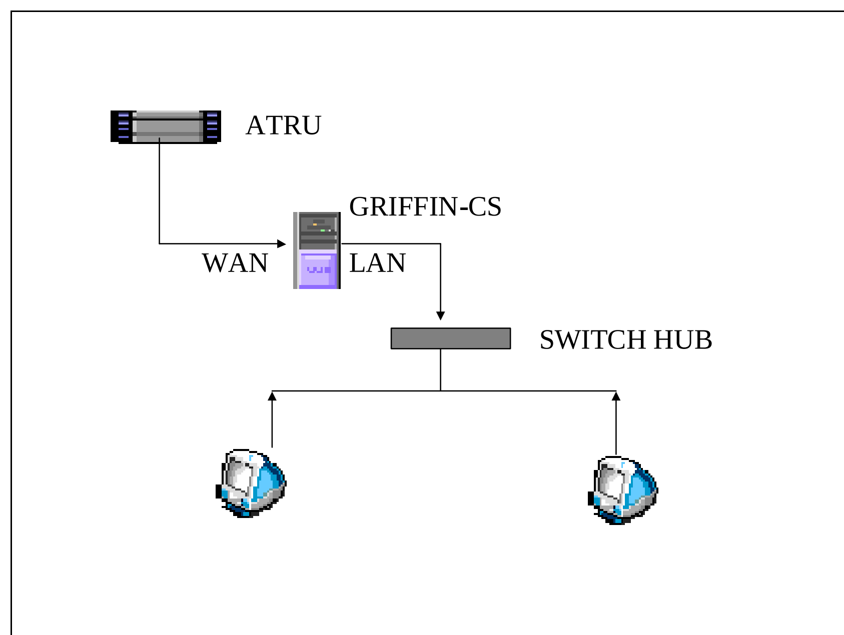
主機電源啓動時，請勿將晶片直接從 IDE 插槽移除，如因此造成晶片損壞，本公司蓋不負責。

系統架構說明

目前 GRIFFIN-CS2 可以支援下列 3 種網路架構規劃

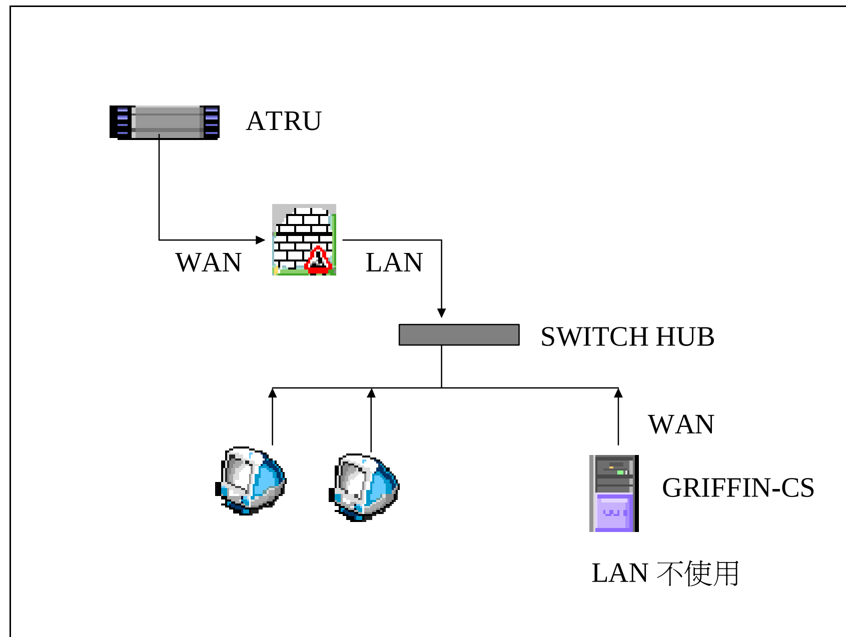
網路閘道架構（NAT 分享）

NAT 分享架構適用狀況爲公司無防火牆的狀況，企業希望以 GRIFFIN-CS2 負責公司防火牆、網頁、郵件、DNS 等伺服器服務，便可以採取此一架構。



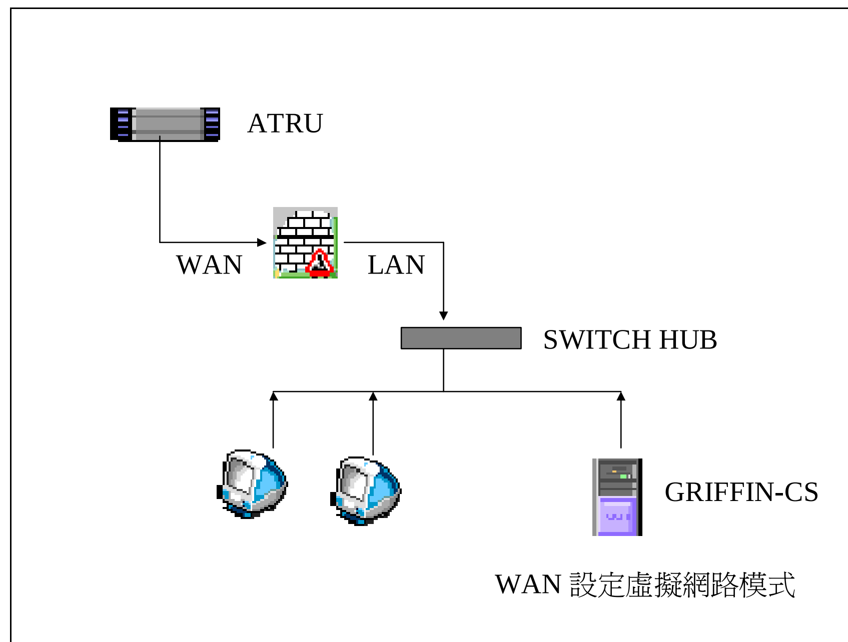
內部單一網路卡架構

內部單一網路架構適用狀況為公司已有防火牆，企業希望以 GRIFFIN-CS2 作為內部的伺服器，並使用一般網路卡，此時 LAN 將不使用，而以 WAN 作為內部網路位置，並由既有防火牆作**位置對應【IP MAPPING】或埠號對應【PORT MAPPING】**，作公司網頁、郵件、DNS 等伺服器服務，便可以採取此一架構。



虛擬網路架構

內部單一網路架構適用狀況為公司已有防火牆，企業希望以 GRIFFIN-CS2 作為內部的伺服器，並使用兩片 INTEL SERVER 網路卡，而以 WAN 作為內部網路位置，並設定虛擬網路模式後，並由既有防火牆來作**位置對應【IP MAPPING】或埠號對應【PORT MAPPING】**，作公司網頁、郵件、DNS 等伺服器服務，便可以採取此一架構。



系統安裝管理程序

本機器的內定出廠網路位置爲如下表

項目	網路位置
第一片網路位置	210.241.254.51
第一片網路遮罩	255.255.255.248
第二片網路位置	192.168.1.1
第二片網路遮罩	255.255.255.0

所以請先調整內部電腦網路設定至相同網路區段，如網路位置爲 192.168.1.2-250 任一個網路位置，確認好管理機器網路位置後，開啓 Internet Explorer，鍵入

http://192.168.1.1:10001/

輸入管理者：admin
管理者密碼：admin（預設）

即會出現 GRIFFIN-CS2 管理介面畫面



GRIFFIN-CS2 管理設定共分八大項如下

- GRIFFIN 資訊
- 系統設定
- 網路設定精靈
- 安全設定
- 伺服器服務設定
- 備份與還原
- 系統監測
- 紀錄檔檢視

下面各章節便依各管理設定下去介紹

注意

GRIFFIN-CS2 是採取系統與資料硬碟分離的設計概念，所以會自動偵測目前系統有無資料硬碟，如發現無資料硬碟則管理者將無法進入本畫面首頁，管理介面會顯示錯誤。

當 GRIFFIN-CS2 偵測到資料硬碟爲新的狀態，則會自動抓取目前資料硬碟的型號及空間容量大小，並請管理者完成資料硬碟格式化的工作，當按下確定格式化鍵時，系統會自動完成整個新資料硬碟的格式，並重新啓動系統，完成整個系統初始化的工作。



GRIFFIN 資訊

GRIFFIN 資訊能夠讓管理者能夠輕易的了解目前系統的一些資訊，其細分爲四個部份主機資訊、伺服器服務狀態、硬碟狀態、系統更新及關於，分別說明如下

主機資訊

會顯示如下資訊

主機名稱	這臺主機的名稱，預設爲”griffin”
主機網域全名	這臺主機的網域名稱，預設爲”griffin.localdomain”
連線方式	這臺主機的網路連線方式，有動態連線及固定連線，預設爲”固定連線”
外部網路位置	這臺主機的網路設定位置，預設爲 210.241.254.51
內部網路位置	這臺主機的網路設定位置，預設爲 192.168.1.1

當使用虛擬網路功能時，連線方式會出現虛擬網路種類

處理器	目前處理器的速度
記憶體	目前記憶體的容量

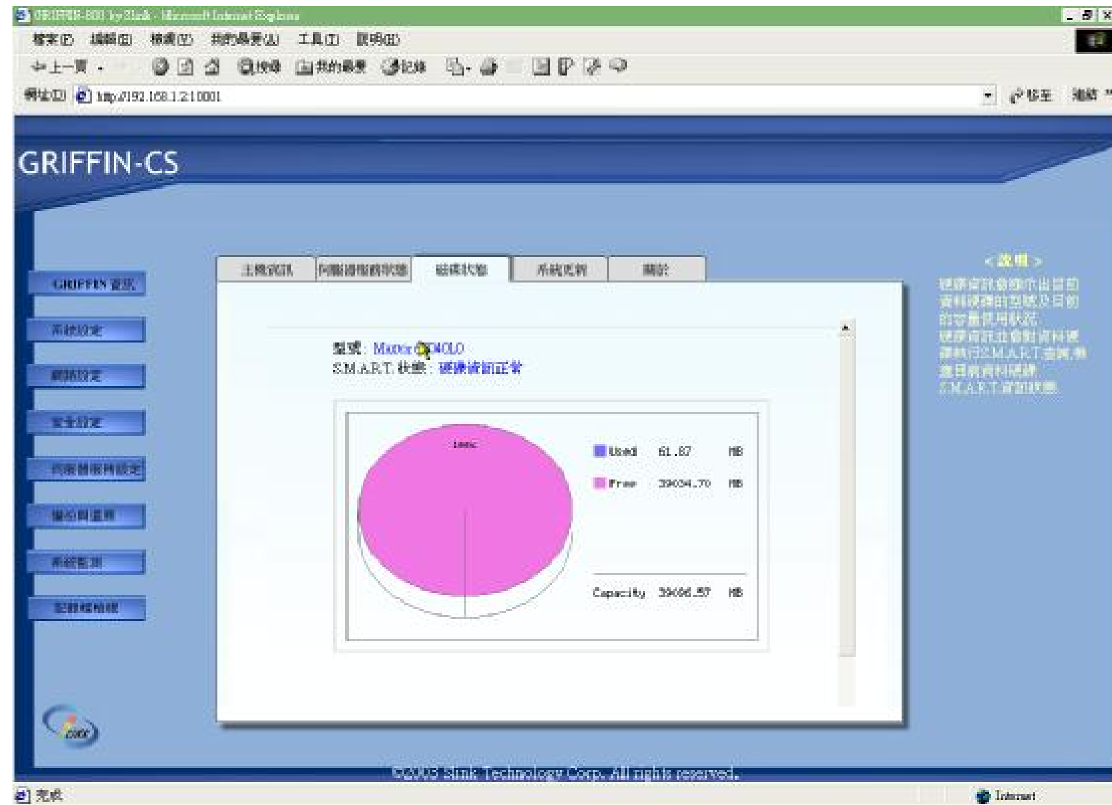
伺服器服務狀態

會顯示出目前 GRIFFIN-CS2 所提供的網路伺服器狀態，有無執行，管理者可輕易從圖示中得到訊息。

	表示伺服器執行中
	表示伺服器已停止

硬碟資訊

會顯示出目前資料硬碟的型號、容量、及 S.M.A.R.T.狀態



注意

SMART 偵測正常為綠色正樣，當出現上面圖片紅色字樣時，表示資料硬碟可能會在近期損壞，請記得立即做好備份，並準備備用資料硬碟作為替換用。

系統更新

GRIFFIN-CS2 提供智慧型的線上更新功能，它會自動檢查目前晶片的更新狀態，自動顯示尚未安裝的更新檔，讓管理者能輕易的從網路上下載 GRIFFIN-CS2 更新檔完成系統更新。

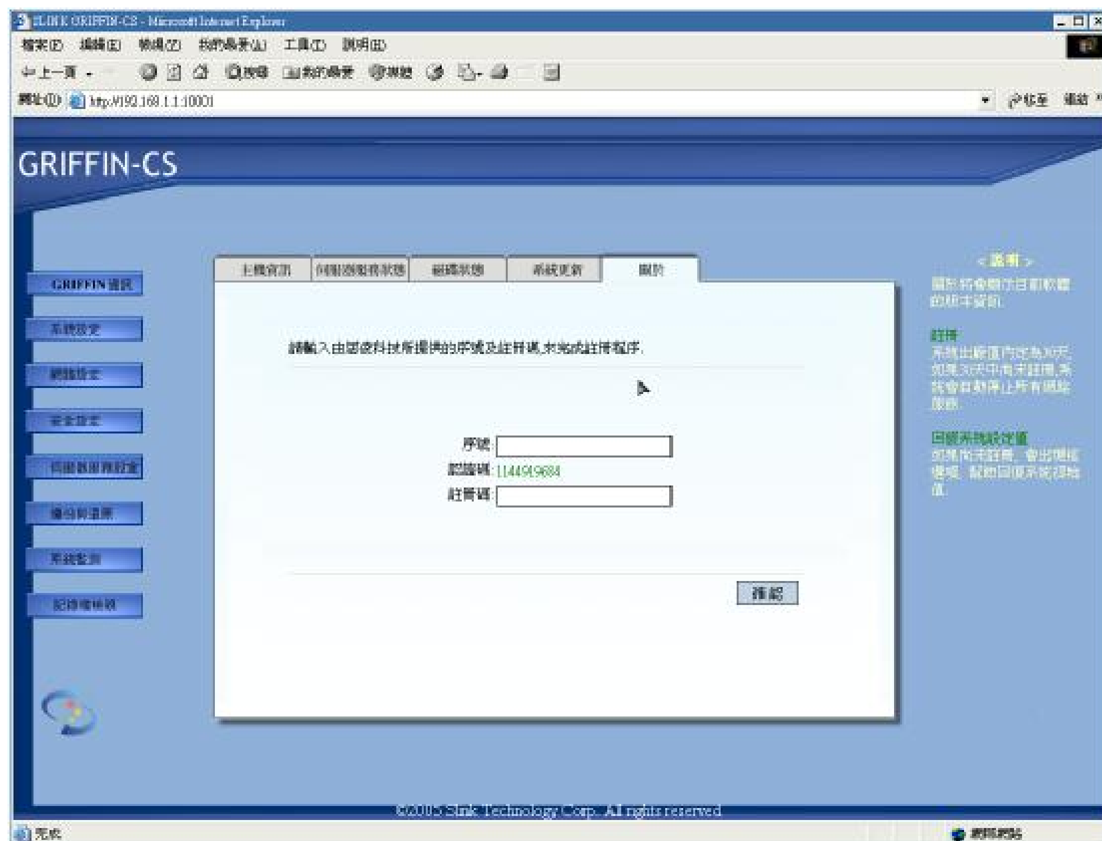
GRIFFIN-CS2 並可設定定期更新取得更新資訊，讓管理者可以在第一時間由郵件得知有無新的更新檔，以在第一時間完成系統更新，所有的系統更新資訊皆會記錄在系統記錄檔中。

注意

當你要使用系統更新時，其 GRIFFIN-CS2 的防火牆如果有啓動，請記得 FTP 服務請務必要允許通過。

關 於

這部份會顯示相關的版權宣告及註冊資訊，本機器從開機算起會有 30 天的試用期，如你已經購買，請上網 http://www.slink.com.tw/reg/輸入序號及下圖綠色字樣的認證碼，以取得註冊碼，取得後請將產品序號及註冊碼填入註冊，完成後以後則只會顯示產品序號，也相當感謝企業購買本產品。



注 意

未完成註冊時會有一個回復系統初始值的功能，按此功能會將 GRIFFIN-CS2 上的資料全部刪除，請小心使用。

認證碼每次重新開機後皆不一樣，所以請取得註冊碼後立即完成註冊，如果尚未完成註冊前，又重新開機，則請再上網取得註冊碼一次。

註冊完成後 GRIFFIN-CS2 會對網路卡做鎖定的動作，如網路卡發生損壞，換新網卡後，將會導致無法進入管理介面，此時請與思凌科技或思凌科技經銷商聯絡，以協助處理。

系統資訊

系統設定爲方便管理者處理系統相關的功能，其細分爲七個部份，管理者密碼變更、管理者資訊設定、使用者管理、時間日期設定、系統效能管理、UPS 設定及系統開關機，分述如下

管理者密碼變更

這功能能提供管理者輕易的變更管理介面的登入密碼及使用者端系統的密碼，如管理者是第一次變更 admin 系統帳號，請在舊密碼欄輸入預設密碼 admin，而如管理者第一次變更 umaster 系統帳號，請在舊密碼欄輸入預設密碼 umaster，再輸入兩次你要變更的密碼，再按下確認即可。

帳號名稱	說明
admin	GRIFFIN-CS2 管理系統登入帳號
umaster	GRIFFIN-CS2 使用者系統登入帳號

管理者信箱設定

這功能提供管理者設定管理者個人的信箱，系統會將所有與系統有關的訊息，如網路資訊，備份資訊，郵寄至這個信箱，讓管理者能夠很快的了解 GRIFFIN-CS2 所發生的狀況。

管理者亦可以在此設定管理版本語言及時區。

思凌科技的系統偵測機制會根據系統的狀態，持續發送警示，這裡管理者可以設定連續警示發送的次數。

基本上這個帳號建議不要使用由 GRIFFIN-CS2 建立的帳號，因爲如果設定爲 GRIFFIN-CS2 的帳號時，管理者將無法得知無資料硬碟時的警告。

使用者管理

使用者管理是讓管理者可以新增、批次新增、修改及刪除郵件帳號及網路登入帳號，畫面如下



當管理者要新增一位使用者時，請按下新增使用者，這時會跳出一使用者新增視窗，要管理者填入各欄位，欄位說明如下

名稱	輸入所要建立的郵件使用者帳號，如你想一位叫 service@your-domain 的帳號，你便鍵入 service 即可。
密碼	輸入這位使用者密碼
確認密碼	再次確認密碼
Windows 目錄權限	參下面說明
郵件轉寄	如果這個帳號需傳寄信件給其他人，請選擇允許，在後面郵件轉寄設定中，管理者便可以設定轉寄，反之則無法設定郵件轉寄。 而當你選擇轉寄時，可以選擇是否保留一份郵件給這位使用者，如欲保留則請勾選保留，否則郵件一轉寄，便不會保留一份給這位使用者
郵件空間限制	使用的的郵件空間配額限制，如超出設定值，則系統會在 7 天後自動刪除超過的空間，目前最大限制為 99999MB。
說明	使用者的說明

GRIFFIN-CS2 內定 5 種使用者屬性，當你設定好 SAMBA 服務資訊，以及啓動這項服務時，你便可透過網路芳鄰來存取 GRIFFIN-CS2 這臺機器的目錄，包含網頁、FTP 目錄及備份等，相當方便管理者做任何管理及網路服務設定。

下表為各網路芳鄰目錄所需的 windows 目錄權限對應

webpage_dir	全部目錄、網頁目錄
cgi-bin_dir	全部目錄、CGI 程式目錄
ftp_dir	全部目錄、FTP 目錄
Backup	全部目錄、備份目錄

注意

當使用者設為網頁目錄權限時，其 FTP（包含共用目錄模式及個人目錄模式）及網路硬碟登錄後皆會到/hom/http/html 這個目錄。

當使用者設為 FTP 目錄權限時，其 FTP（包含共用目錄模式及個人目錄模式）及網路硬碟登錄後皆會到/hom/ftp 這個目錄。

名稱請勿以數字為第一個字元，如”1test”不然會出現錯誤

批次新增使用者帳號

目前 GRIFFIN-CS2 支援 3 種批次新增使用者的方式，分述如下

- 前置碼+循序數字

  前置碼可輸入 stud，開始編號輸入 1，結束編號數入 3，位元編號選擇 5，則會產生如下的帳號

  stud00001

  stud00002

  stud00003

- 前置碼+循序數字+循序數字

  前置碼可輸入 stud，第一層開始編號輸入 1，第一層開始編號輸入 2，位元組輸入 2，第二層開始編號輸入 1，第二層開始編號輸入 3，位元組輸入 5，則會產生下列的帳號

  stud0100001

  stud0100002

  stud0100003

  stud0200001

  stud0200002

  stud0200003

- Slink 自訂格式匯入

  思凌科技目前提供的自訂格式為下

  名稱　密碼　郵件限制(MB)

  每個欄位請以空白隔開，其中郵件限制如果不限制則請設 0，如過超過 100 則會以 100 下去計算

  當要使用自訂格式匯入時，因系統會去/home/admin/account 這個目錄抓取檔案，所以請記得先啓動網路硬碟的功能，並以 admin 的帳號登入，在網路硬碟中編輯自訂格式檔案。

- 批次刪除

  所有批次新增，皆會記錄與系統，供管理者做批次刪除。

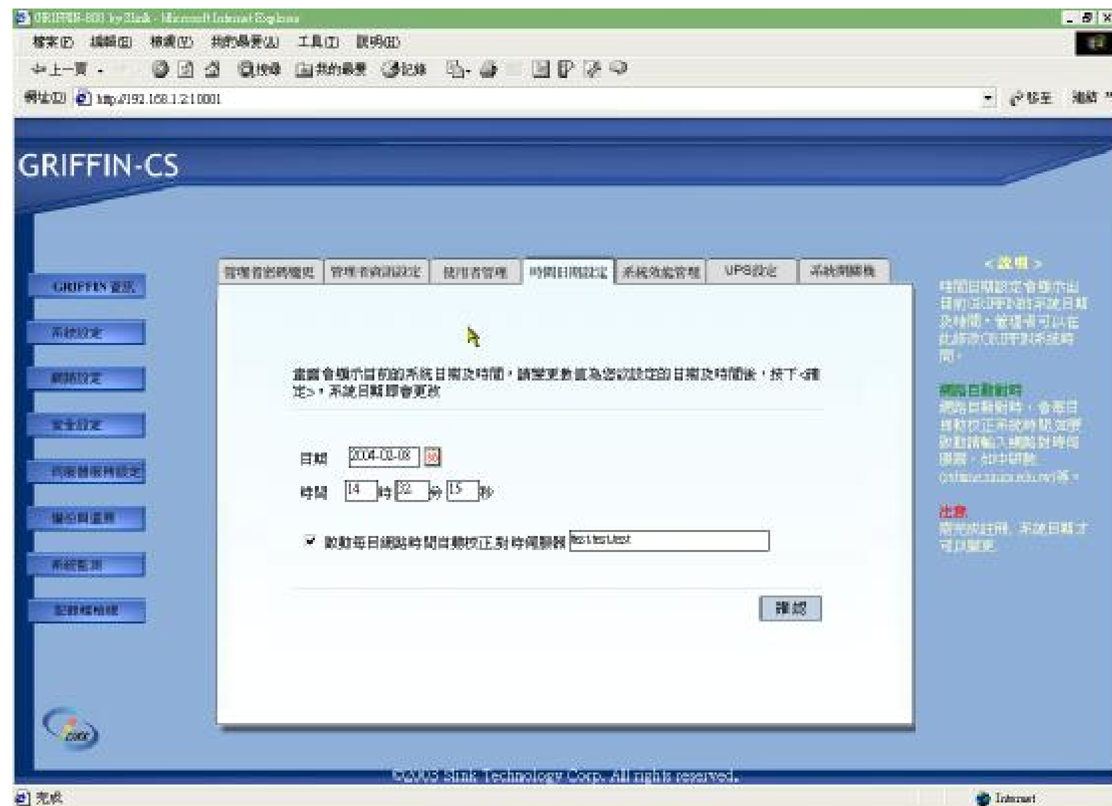
以上各批次新增方式，在條件設定後，皆先會出現檢視畫面，如果檢視無誤，則可按下完成，完成批次新增。

使用者報表

管理者可以設定要檢視個別使用者或全部使用者的報表，使用者報表會將使用者的全部資訊，包含個人檔案目錄、有無信件未收等細部資訊，郵寄一份至管理者信箱。

時間日期設定

時間日期設定會顯示出目前的系統所設定的時間，管理者亦可以調整畫面上的時間，按下確認後系統時間便會重新設定成管理者所輸入的時間。



注意：

當您尚未完成 GRIFFIN-CS2 的註冊步驟時，是無法變更系統日期。

GRIFFIN-CS2 亦支援網路 NTP（Network Time Protocol）對時功能，管理者能設定網路自動對 NTP 伺服器對時。

常見的網路 NTP 伺服器如下

time.chttl.com.tw

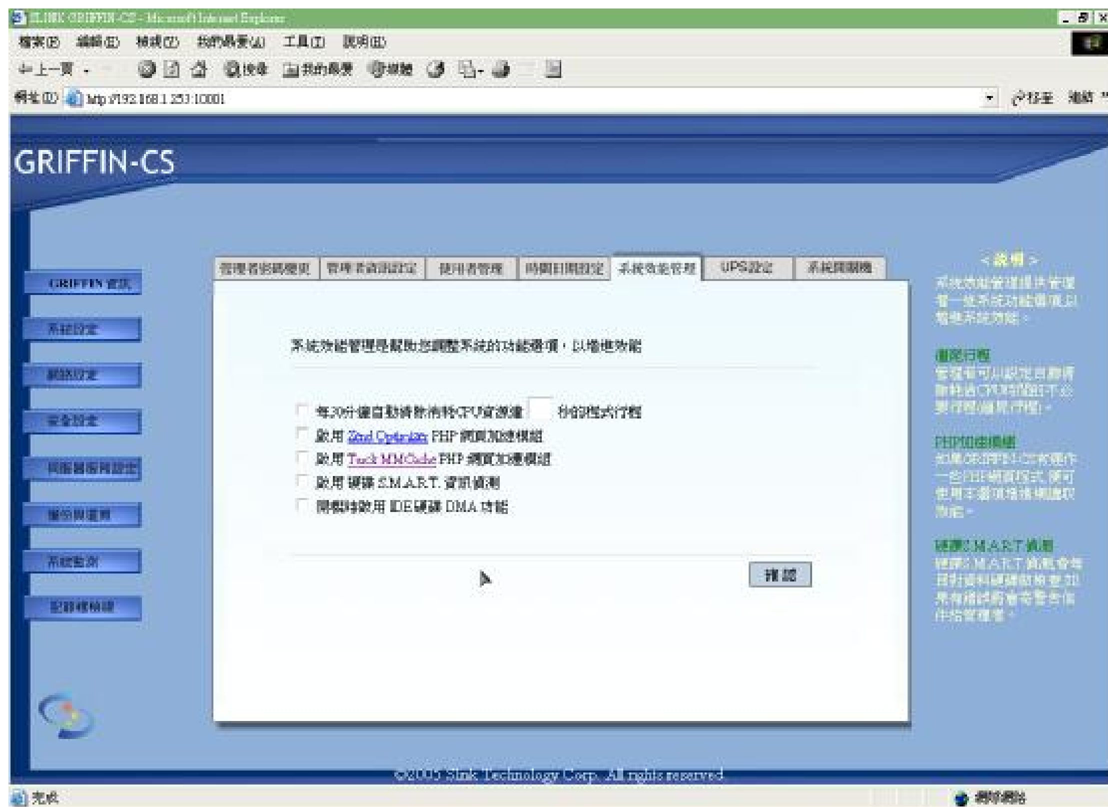
stdtime.sinica.edu.tw

ntp-1.nctu.edu.tw

clock.chrrl.com.tw

系統效能管理

系統效能為一些可以增進系統效能的選項，目前可以幫助你自動清除所謂的僵屍行程，及啓動網頁 PHP 加速模組，以免有問題的行程耗掉 GRIFFIN-CS2 的資源，並可增進 PHP 網頁的存取速度，目前可以支援 Zend Optimizer 或 eAccelerator，管理者可以針對需求擇一選擇（如有使用 WEBMAIL 等功能，建議使用）。



何謂僵屍行程（Zombie）？

因為 GRIFFIN-CS2 本身是一台網路上的伺服器，系統上有來自各地的連線，有時會發生某些處理的主程式已經結束，但是子程序還未完全消除，而這些行程會耗用系統資源，進而影響到系統效能，GRIFFIN-CS2 提供管理者自動清除掉這些行程。

- **S.M.A.R.T 資訊偵測**

  S.M.A.R.T（Self-Monitoring, Analysis and Reporting Technology）硬碟自我偵測分析及報告技術，它會去詢問目前硬碟的狀態，並產生資訊，當管理者啓用這功能時，GRIFFIN-CS2 每天會去自動執行詢問硬碟的工作，並在有問題時郵寄錯誤訊息給管理者。

- **Zend Optimizer PHP 網頁加速模組**

  GRIFFIN-CS2 支援 Zend（http://www.zend.com/）的 PHP 網頁加速模組，使用這選項可以幫助您的 PHP 網頁速度加快，並當您的 PHP 網頁有使用 Zend 公司的 PHP 加密軟體加密過後，請務必勾選這個選項才可以正常顯示加密過的 PHP 網頁。

- **eAccelerator PHP 網頁加速模組**

  GRIFFIN-CS2 支援 Zend（http://eaccelerator.net/）的 PHP 網頁加速模組，使用這選項可以幫助您的 PHP 網頁速度加快，並當您的 PHP 網頁有使用 eAccelerator 加密過後，請務必勾選這個選項才可以正常顯示加密過的 PHP 網頁，如思凌科技 PEGAS 網路購物商店軟體 1.3 版以後。

注意!!

系統會自動判定目前硬碟的種類，當您硬碟爲 IDE 硬碟時，才會出現
開機時啓用 IDE 硬碟 DMA 功能
的選項供您選擇

UPS 設定

GRIFFIN-CS2 支援各廠牌的 UPS，管理者可以相當容易的設定支援，詳細的設定值可以直接上網查詢，思凌科技持續提供最新的 UPS 支援廠牌設定值。

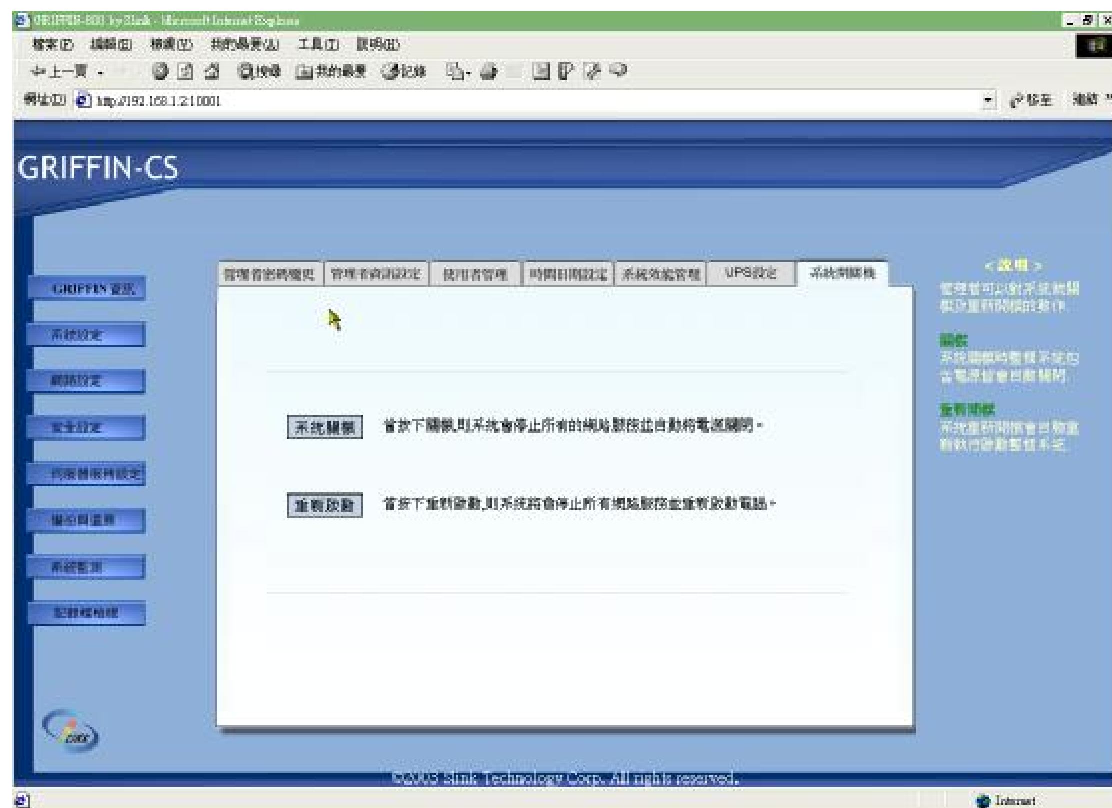


系統開關機

系統開關機能讓管理者在遠端 GRIFFIN-CS2 的關機或重新啟動。

關機：關閉這台 GRIFFIN-CS2，並會自動將電源關閉

重新啟動：重新啟動 GRIFFIN-CS2



網路設定

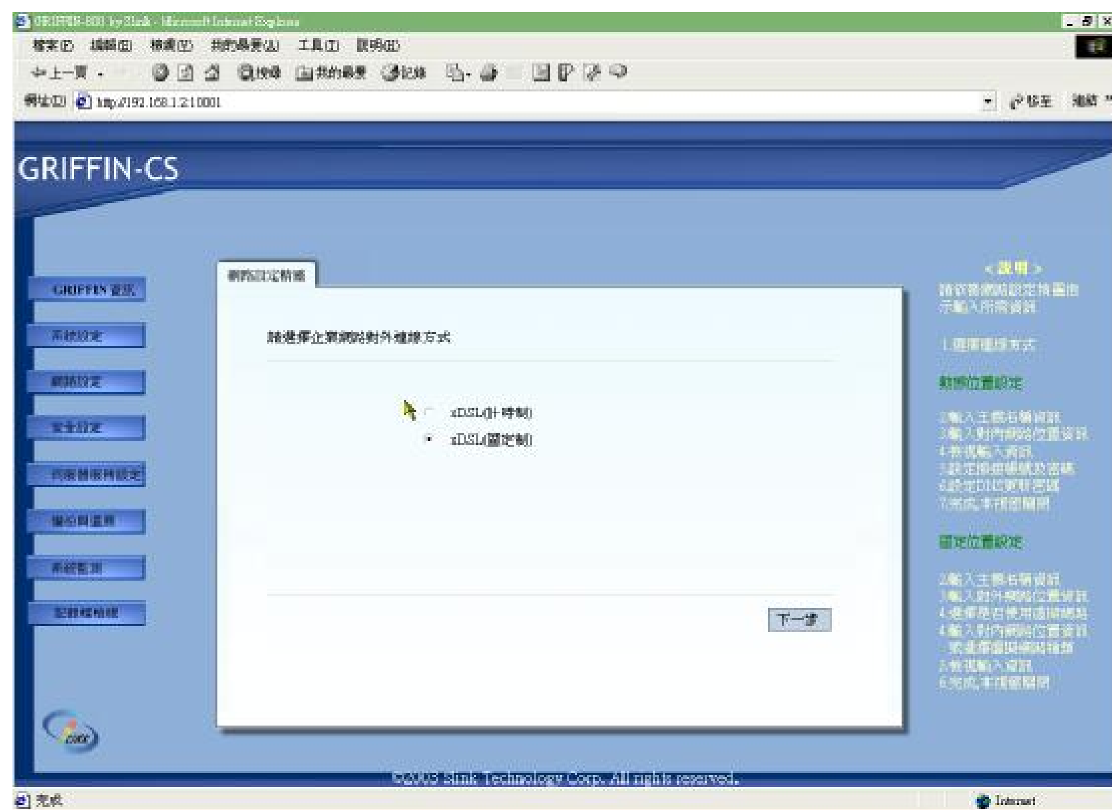
GRIFFIN-CS2 提供兩個功能選項讓管理者可以相當容易的完成 GRIFFIN-CS2 的網路設定，其分別為網路設定精靈及的進階設定

網路設定精靈

網路設定精靈為思凌科技為了方便使用者設定修改這台 GRIFFIN-CS2 的網路位置（IP ADDRESS）所特別設計的介面，管理者只要依著設定畫面，填入所需資訊，幾可輕鬆地完成網路位置的設定，GRIFFIN-CS2 網路設定精靈的設定步驟如下

選擇企業網路連線方式

GRIFFIN-CS2 支援固定網路位置架設及動態網路位置架設，管理者可以依企業實際的連線方式去做設定，不一樣的選擇會出現不一樣的精靈步驟



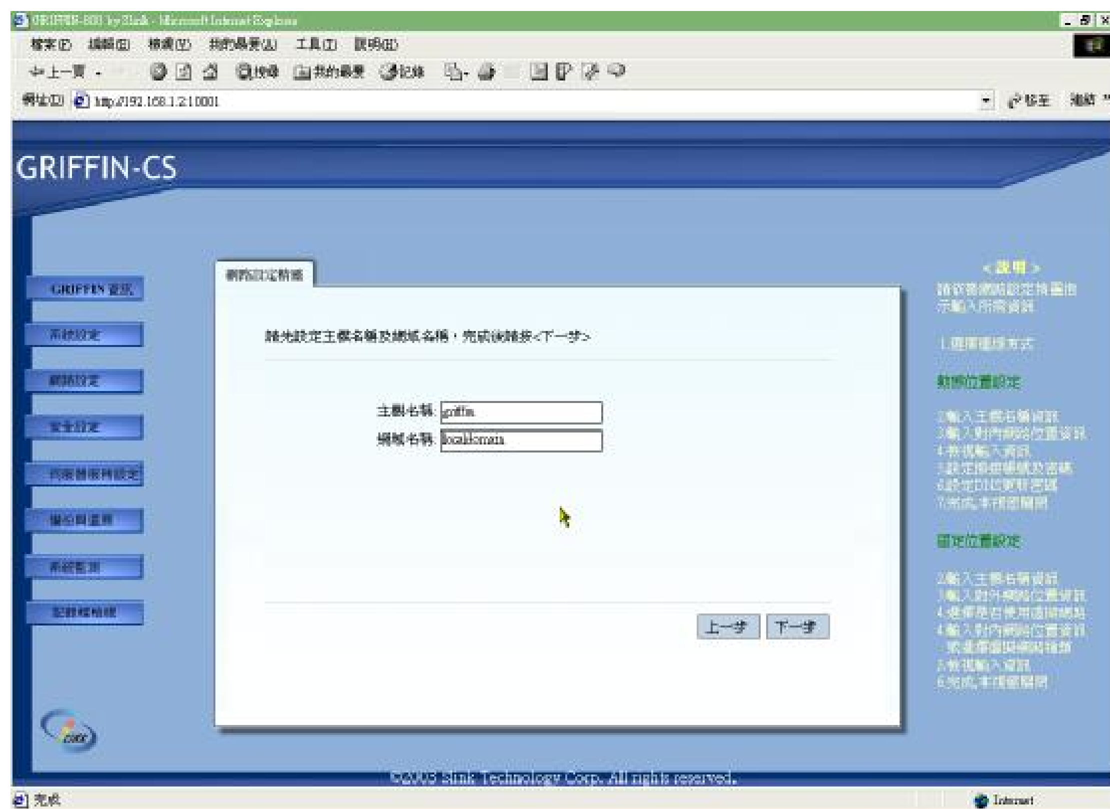
注意：

當企業選擇計時制 xdsl 作爲連線方式時，DNS 並無法正常的對應，因爲目前 TWNIC 在做動態 DNS 配置時，並不會再往下詢問企業的 DNS，所以並無法去解析管理者所定義的 DNS 記錄。

基本上郵件伺服器在計時制 xdsl 也可正常執行，不過當對方的防火牆會做 IP 防假冒檢查時，企業的郵件可能會被退回，因爲企業的網路位置並無法被防火牆反解，對方防火牆有可能會認爲企業的郵件位置爲假，而退回企業的郵件伺服器的信件，所以這點請企業相當注意。

輸入主機名稱資訊

這邊請輸入管理者所要這台 GRIFFIN-CS2 的主機名稱，內定爲 griffin，當然管理者也可以取自己較喜愛的名稱，網域名稱部分則請輸入貴公司在網域註冊中心所申請的網域名稱，內定爲 localdomain，像思凌科技所申請的網域名稱爲 slink.com.tw，則輸入 slink.com.tw。

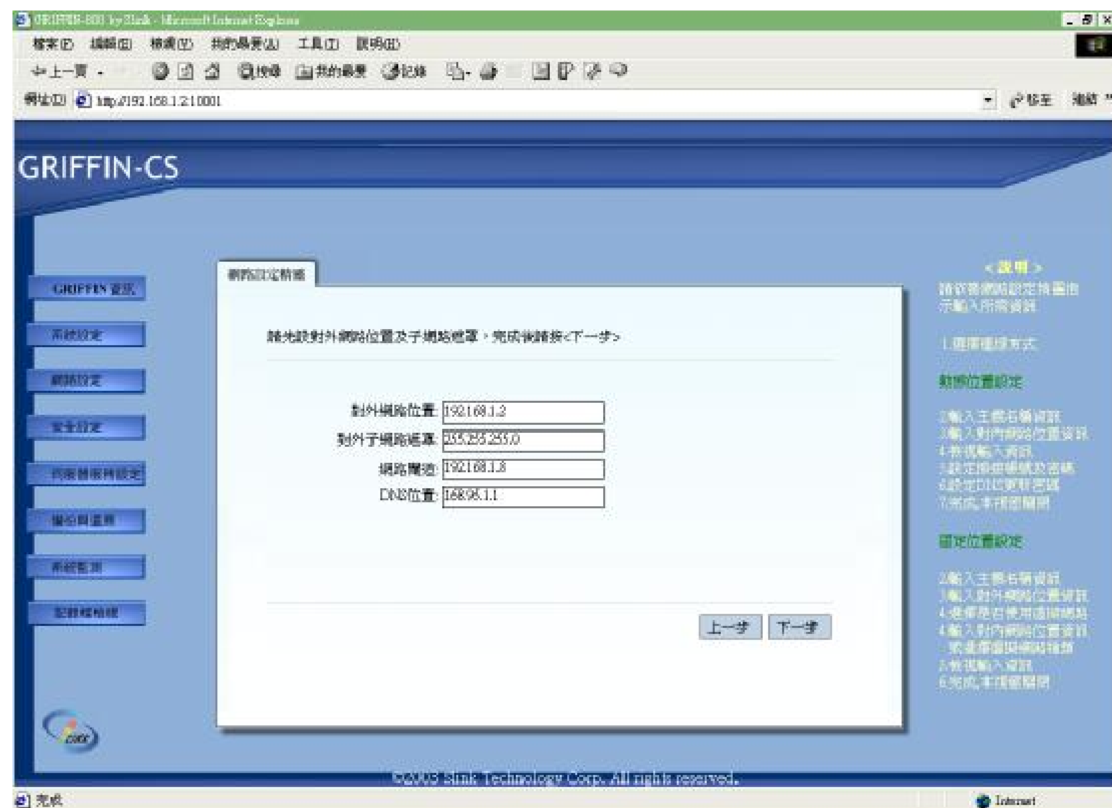


注意

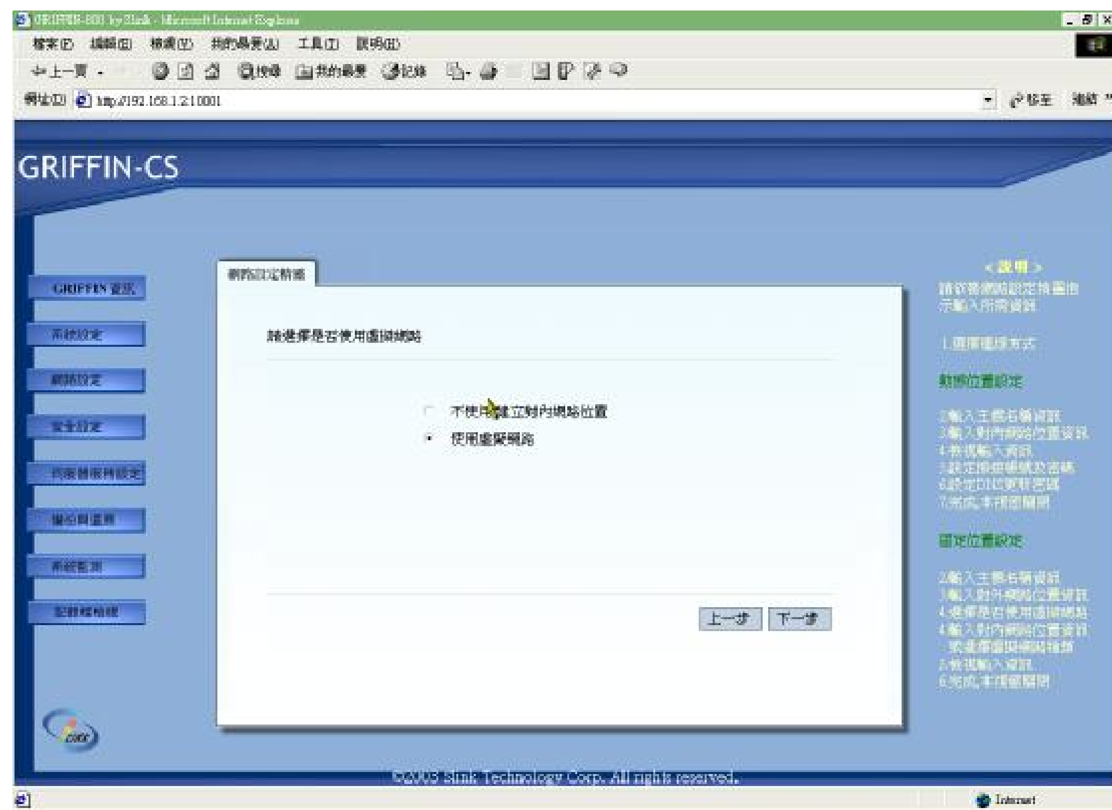
如果 GRIFFIN-CS2 本身也規劃作爲 DNS 伺服器，則主機名稱請勿取與 DNS 常用名稱一樣，如 www、mail、ftp 等，以確保 GRIFFIN-CS2 整體服務運作正常。

固定式連線

這邊請輸入管理者所欲設定的外部網路位置，因為 GRIFFIN-CS2 的定位為閘道型伺服器裝置，這裡請輸入一個真實的網路位置，出廠內定值為 210.241.254.51，子網路遮罩得內定值為 255.255.255.248，網路閘道則請輸入貴對外的網路閘道位置，內定為 210.241.254.49，DNS 位置則請修改為提供貴公司網路連線（如 ADSL 等）服務公司所設定的 DNS 位置，內定為中華電信的 DNS 位置，168.95.1.1。



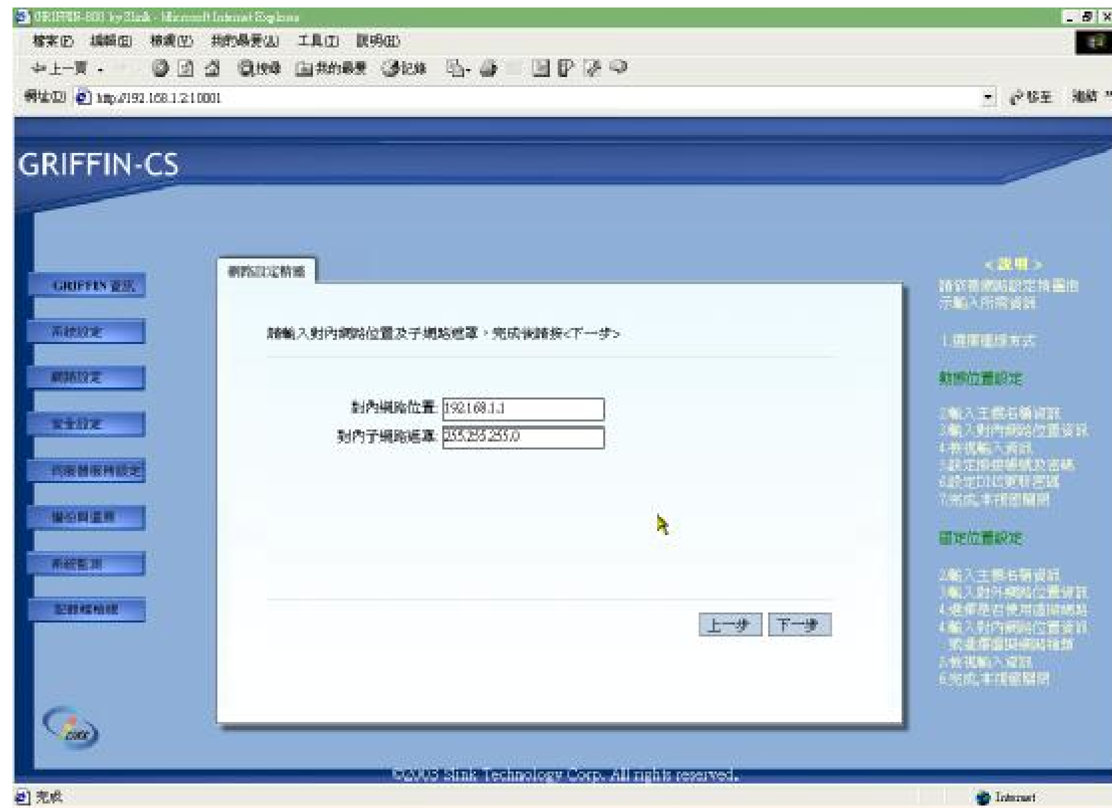
接下來請選擇是否啓用虛擬網路的功能，如果不啓用則自動變爲 NAT 的閘道主機模式，需再設定一個虛擬網路位置給第二個網路卡，如選擇啓用，則第二網路卡則會支援第一網路卡的網路位置，並自動啓用虛擬網路功能。



底下分面說明兩種模式的設定

不啓用虛擬網路

請輸入第二網路卡的網路位置（公司內部的虛擬網路位置），這個網路位置將為本區段的網路閘道位置，系統內定值為 192.168.1.1，網路遮罩為 255.255.255.0



啓用虛擬網路的功能

GRIFFIN-CS2 的虛擬網路的功能，共有四種設定，管理者可以視公司網路環境選擇適當的模式，內定值爲 AFT 模式，不過這裡建議可以選擇 ALB 模式，以達到最佳的網路利用率。



各模式說明

- **n** AFT(雙網路介面容錯備援)模式
  此時 GRIFFIN-CS2 的第二網路卡會處於待命的模式，當第一片網路卡發生錯誤，此待命網路卡便會立即接手第一片網路卡的工作，使得 GRIFFIN-CS2 的網路服務能繼續正常服務

- **n** SFT(雙 SWITCH 容錯備援)模式
  此時 GRIFFIN-CS2 的第二網路卡需接於不同的 SWITCH HUB 上，當其中一台 SWITCH HUP 發生故障時，網路封包會自動從正常的 SWITCH HUB 繼續工作，使得 GRIFFIN-CS2 的網路服務能繼續正常服務

- **ALB(雙網路介面負載平衡) 模式**
  此時 GRIFFIN-CS2 的第二網路卡會繼續服務，並與第一片網路卡平均分配網路的流量，以降低每一片網路卡的負載，減少損毀的機率，其中如果一片網卡損壞，另一片網卡仍能正常的運作，亦具有備援功能，所以建議可以用爲企業設定值。

- **802.3ad(雙網路介面流量匯集,802.3ad)模式**
  此時 GRIFFIN-CS2 的第二網路卡會繼續服務，並與第一片合併網路頻寬，如此時 GRIFFIN-CS2 網路流量頻寬會變成 100Mb+100Mb=200Mb，其中如果一片網卡損壞，另一片網卡仍能正常的運作，亦具有備援功能，不過這個功能需要 SWITCH HUB 亦要支援 802.3ad 的標準，一般而言，INTEL 及 CISIO 的 SWITCH HUB 都有支援。

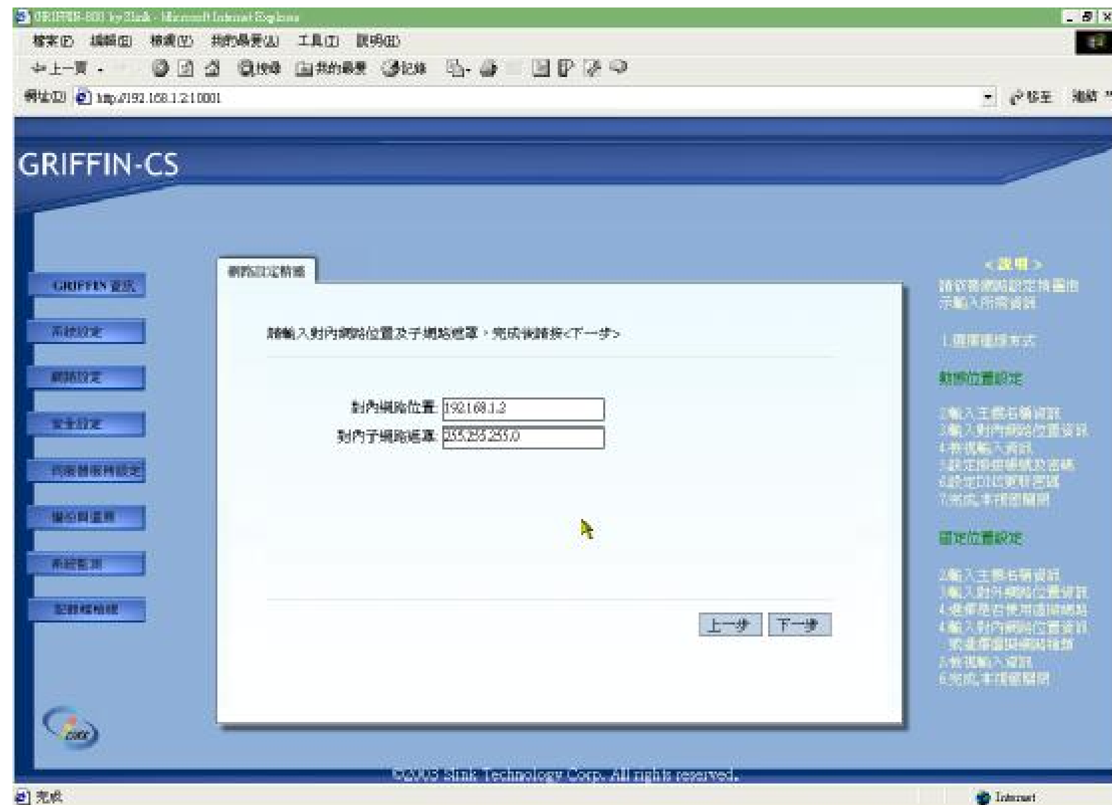
虛擬網路的功能沒有支援動態網路連線，所以如果企業是以撥接式 xDSL 便無法享受到這功能的效能，目前亦支援 BROADCOM 的 VLAN 功能。

接下來會出現檢視畫面，在確認設定值無誤後按下確定，即可完成網路設定，接下來會出現請你關閉視窗的畫面，按下確定後即可完成設定，一分鐘後管理者及可以新的網路位置連線做管理。

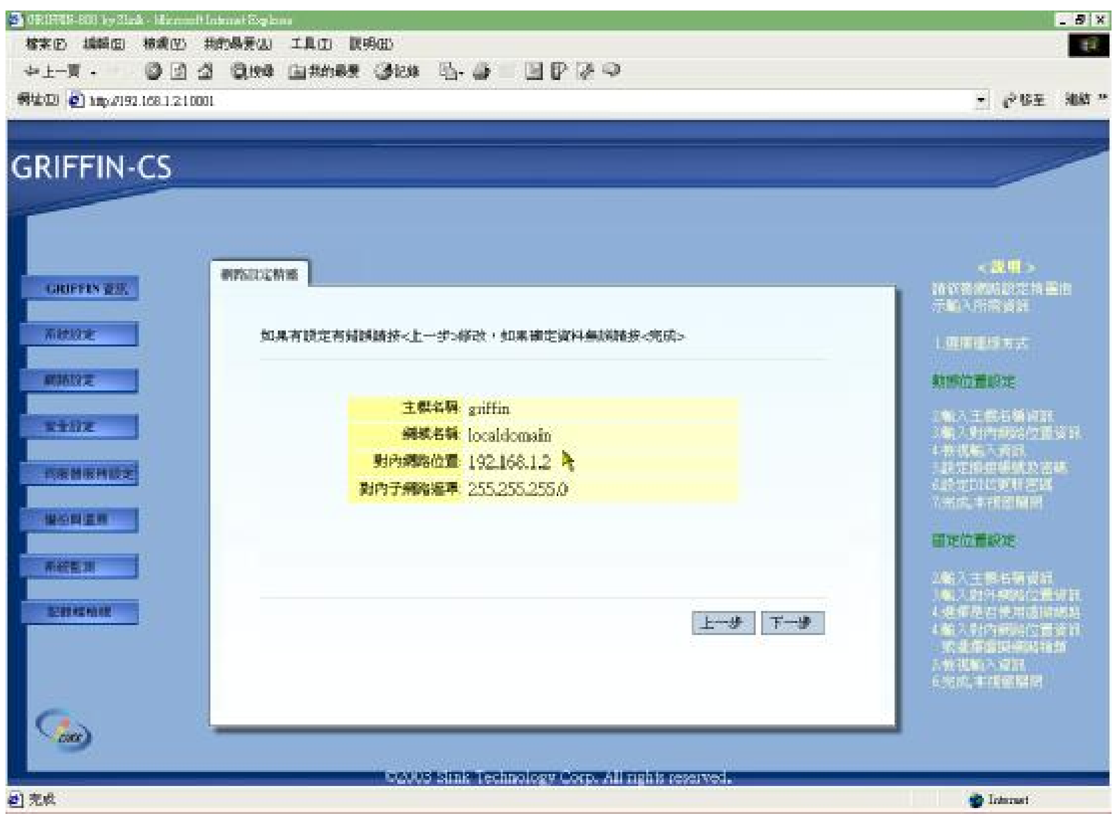


動態網路連線

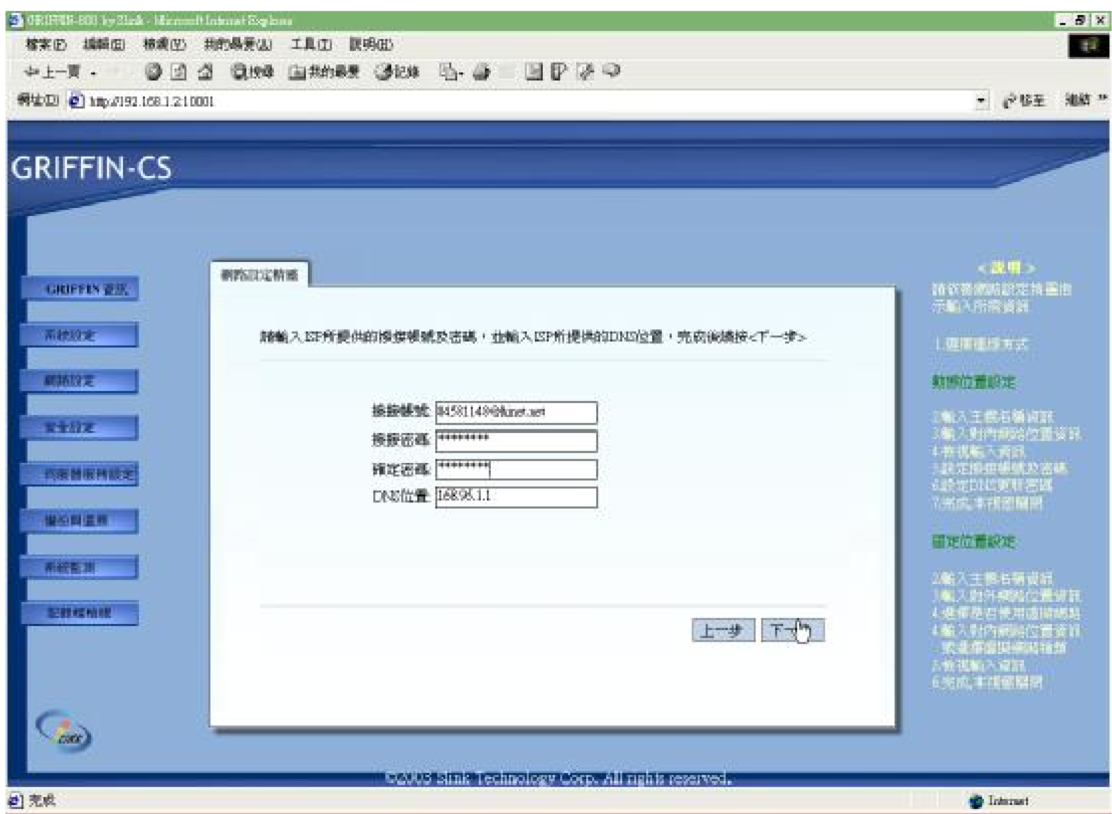
這邊請輸入管理者所欲設定的內部網路位置，因為 GRIFFIN-CS2 的定位為伺服器裝置，所以並不提供 DHCP 自動取得網路位置的方式，所以請為 GRIFFIN-CS2 規劃一個內部固定網路位置，這個位置亦會成為該網路區段的網路閘道，出廠內定值為 192.168.1.1，子網路遮罩得內定值為 255.255.255.0。



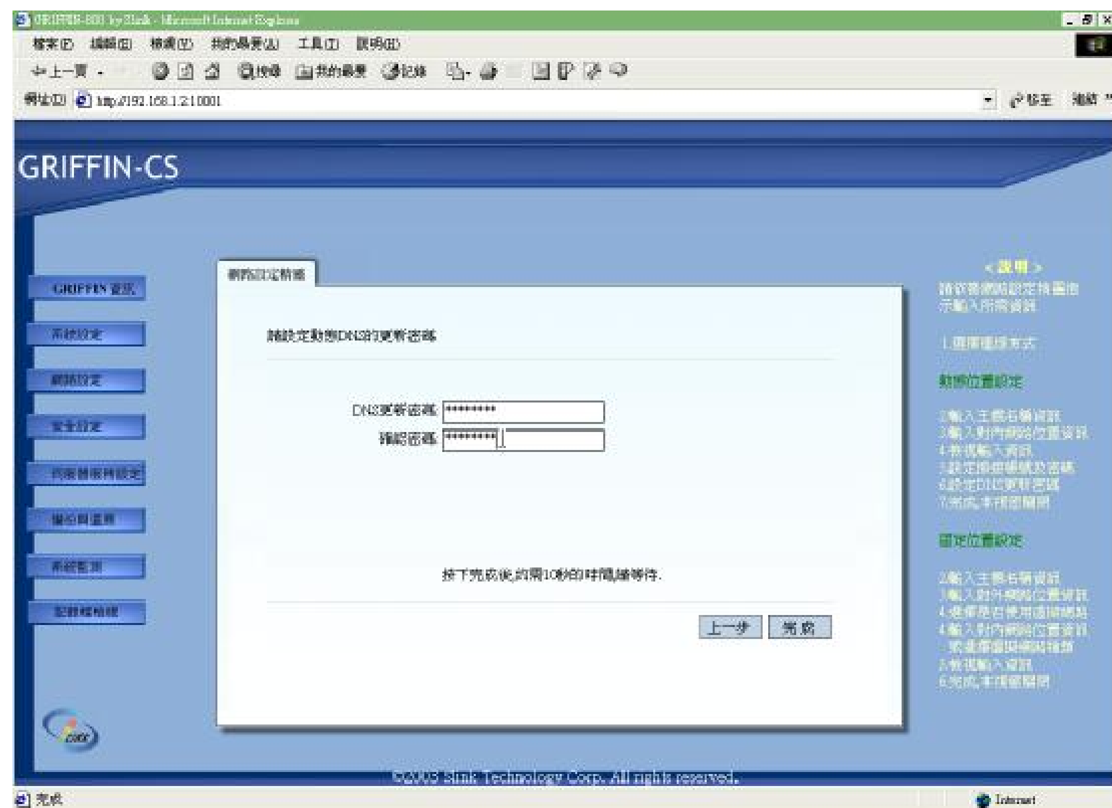
接下來會出現網路檢視畫面



接下來請輸入企業 xDSL 所申請的撥接帳號，密碼及該 ISP 所提供的 DNS 網路位置。



接下來請輸入貴公司申請網域時的動態更新密碼



再來按下確定即可完成設定

DNS 更新

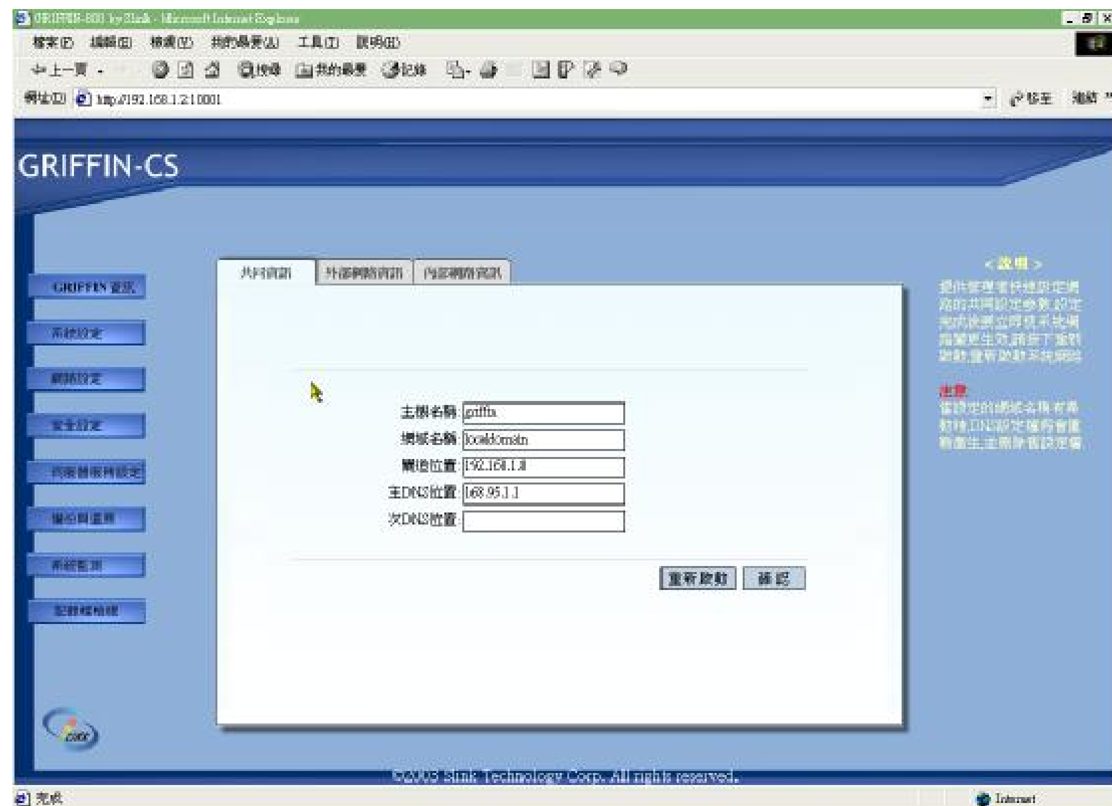
GRIFFIN-CS2 內建的 DNS 更新功能為與財團法人台灣網路資訊中心（TWNIC）所提供，目前各有提供動態 DNS 的網域申請提供商，皆可使用。

進階設定

進階設定提供管理者快速的控制每一個網路參數，其分為三個小項，分別為共同資訊、外部網路資訊及內部網路資訊，分述如下

共同資訊

共同資訊提供管理者快速設定主機名稱、網域名稱、閘道、及主要及次要 DNS 位置，設定完成後請按下確定，不過此時系統網路的真實設定並未變更，如要立即變更系統網路設定，請按下重新啟動，如此 GRIFFIN-CS2 會重新啟動整個網路設定



外部網路資訊

共同資訊提供管理者快速設定外部網路位置及遮罩，設定完成後請按下確定，不過此時系統網路的真實設定並未變更，如要立即變更系統網路設定，請按下重新啟動，如此 GRIFFIN-CS2 會重新啟動整個網路設定



內部網路資訊

內部網路資訊提供管理者快速設定內部網路的網路位置、遮罩、及開機時是否啓動，設定完成後請按下確定，不過此時系統網路的真實設定並未變更，如要立即變更系統網路設定，請按下重新啓動，如此 GRIFFIN-CS2 會重新啓動整個網路設定



如果為支援虛擬網路則此頁面會變為選擇虛擬網路的種類，詳細說明請參第 35 頁，啓動虛擬網路。

安全設定

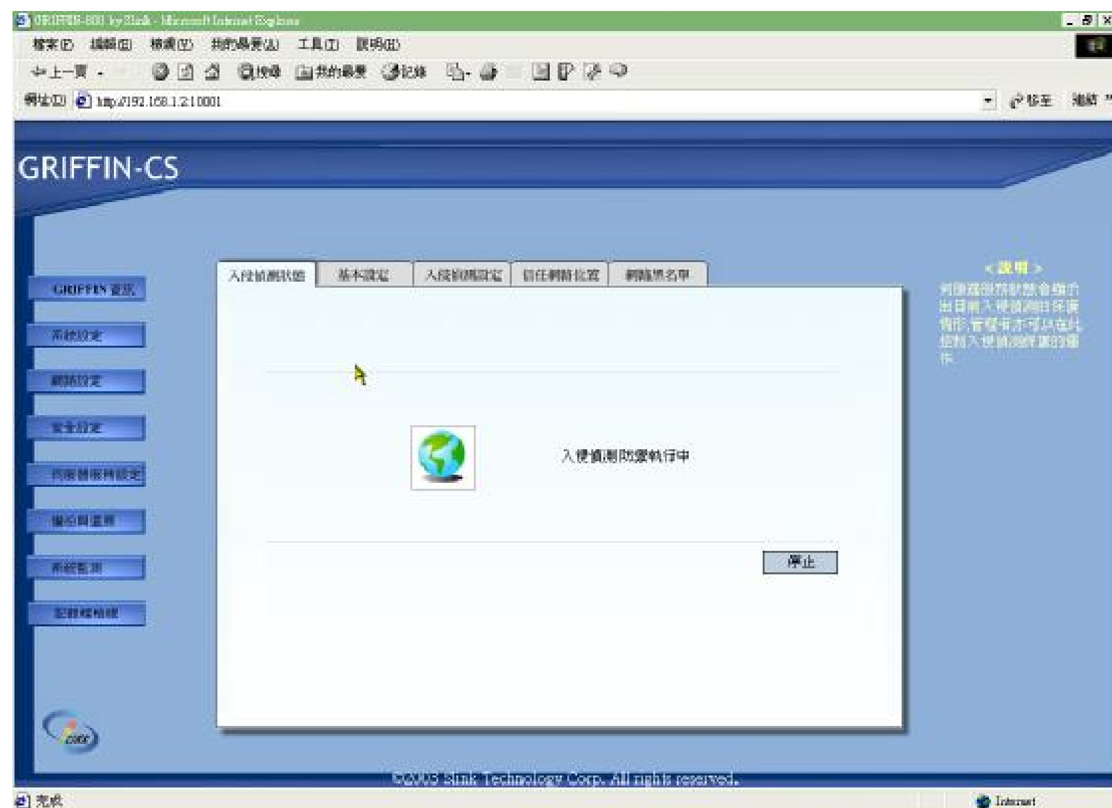
GRIFFIN-CS2 針對網路安全部分，提供企業兩大功能，入侵偵測及防火牆功能，分述如下

入侵偵測設定

GRIFFIN-CS2 內建入侵偵測防禦功能，能在網路攻擊者的攻擊第一步驟主機弱點掃描時，第一時間將網路攻擊者的網路位置紀錄下來，並自動通知防火牆將此網路位置列爲拒絕連線位置，以避免網路攻擊者的下一步攻擊，其共有五小項，分述如下

入侵偵測狀態

讓管理者可以監視入侵偵測的狀態，並在線上控制這項網路服務的是否運作。



基本設定

這裡讓管理者可以設定是否在 GRIFFIN-CS2 開機時自動啓動入侵偵測防護。



其有三種防禦等級，初級、中級及高級，三種等級所做的防禦各不相同，以下爲各等級防禦的埠號範圍。

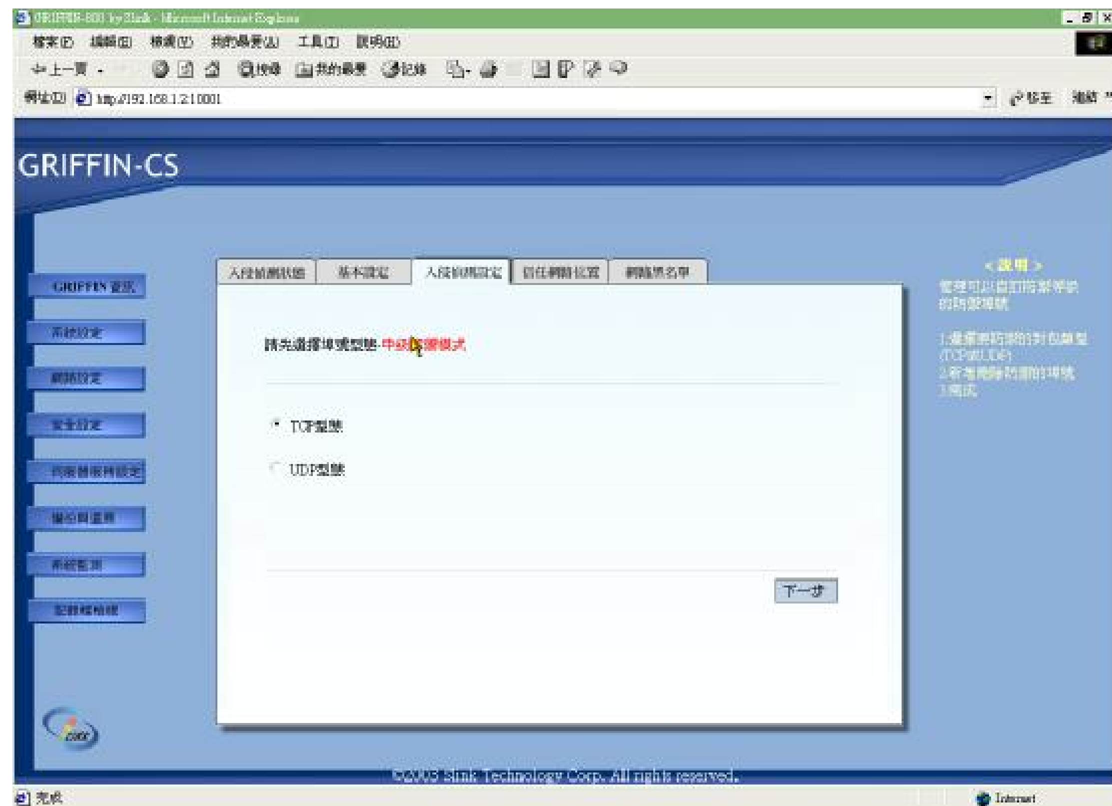
等級	種類	埠號範圍
初級	TCP	1,11,15,110,111,143,540,635,1080,1524,2000,12345,12346,20034,32771,32772,32773,32774,49724,54320
	UDP	1,7,9,69,161,162,513,640,700,32770,32771,32772,32773,32774,31337,54321
中級	TCP	1,11,15,79,111,119,143,540,635,1080,1524,2000,5742,6667,12345,12346,20034,27665,31337,32771,32772,32773,32774,40421,49724,54320
	UDP	1,7,9,69,161,162,513,635,640,641,700,37444,34555,31335,32770,32771,32772,32773,32774,31337,54321
高級	TCP	1,7,9,11,15,70,79,80,109,110,111,119,138,139,143,512,513,514,515,540,635,1080,1524,2000,2001,4000,4001,5742,6000,6001,6667,12345,12346,20034,27665,30303,32771,32772,32773,32774,31337,40421,40425,49724,54320
	UDP	1,7,9,66,67,68,69,111,137,138,161,162,474,513,517,518,635,640,641,666,700,2049,31335,27444,34555,32770,32771,32772,32773,32774,31337,54321

管理者可針對自己認可的安全等級進行設定，以達到自己所認可的網路安全防禦等級。

以上列的設定值爲內定防禦埠號，管理者可以在入侵偵測設定，針對不同的安全等級在進行防禦埠號微調。

入侵偵測設定

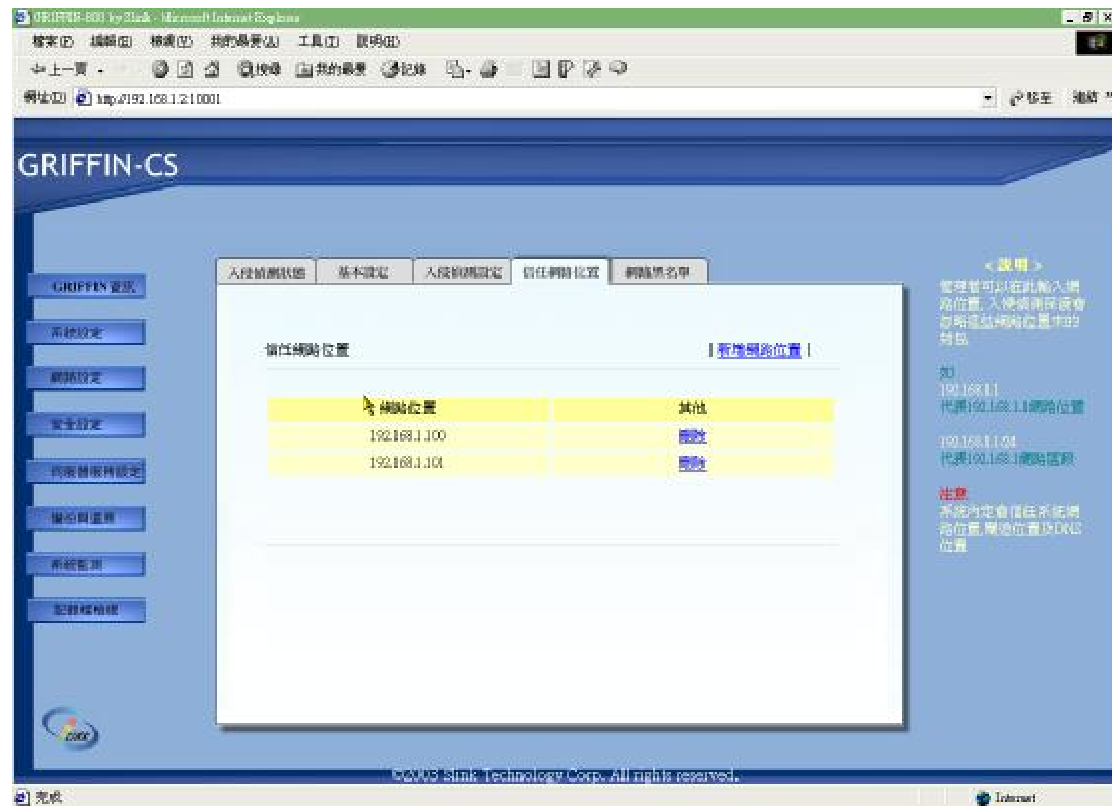
當管理者設定完成基礎的防禦模式後，這個功能可以讓管理者進行所謂的埠號微調。



畫面顯示目前的模式，並請管理者先選擇設定何種網路封包型態，選擇完畢後按下一步，便會呈現出目前這個等級所做的埠號防禦，管理者可以針對自的需求進行新增刪除設定。

信任網路位置

這裡提供管理者設定信任的網路位置，即從這個網路位置來的網路封包一律忽略不做檢查。



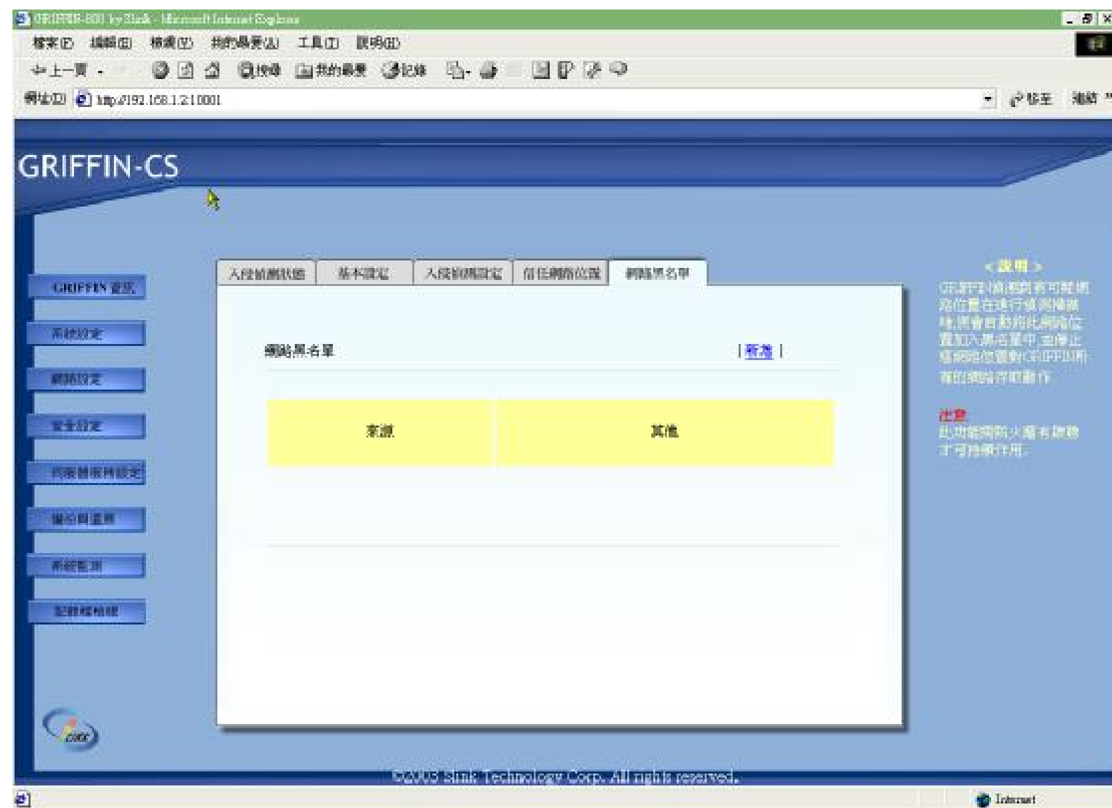
因為入侵偵測系統會針對網路封包進行網路偵測，所以有時會耗掉相當的系統及網路資源，所以針對管理者認為安全的網路位置可以忽略不檢查，以增加信任網路位置的網路效率。

系統內定在啓動時會將系統的網路位置、閘道位置及 DNS 位置視為安全的網路位置，不做檢查。

請特別注意，信任的網路位置是以**網路位置**為主要的設定值，所以管理者必須輸入網路位置，如 192.168.1.1 或代表整個網路區段的位置，192.168.1.0/24 等。

網路黑名單

管理者可以在此設定哪一個網路位置 GRIFFIN-CS2 一律拒絕網路連線。



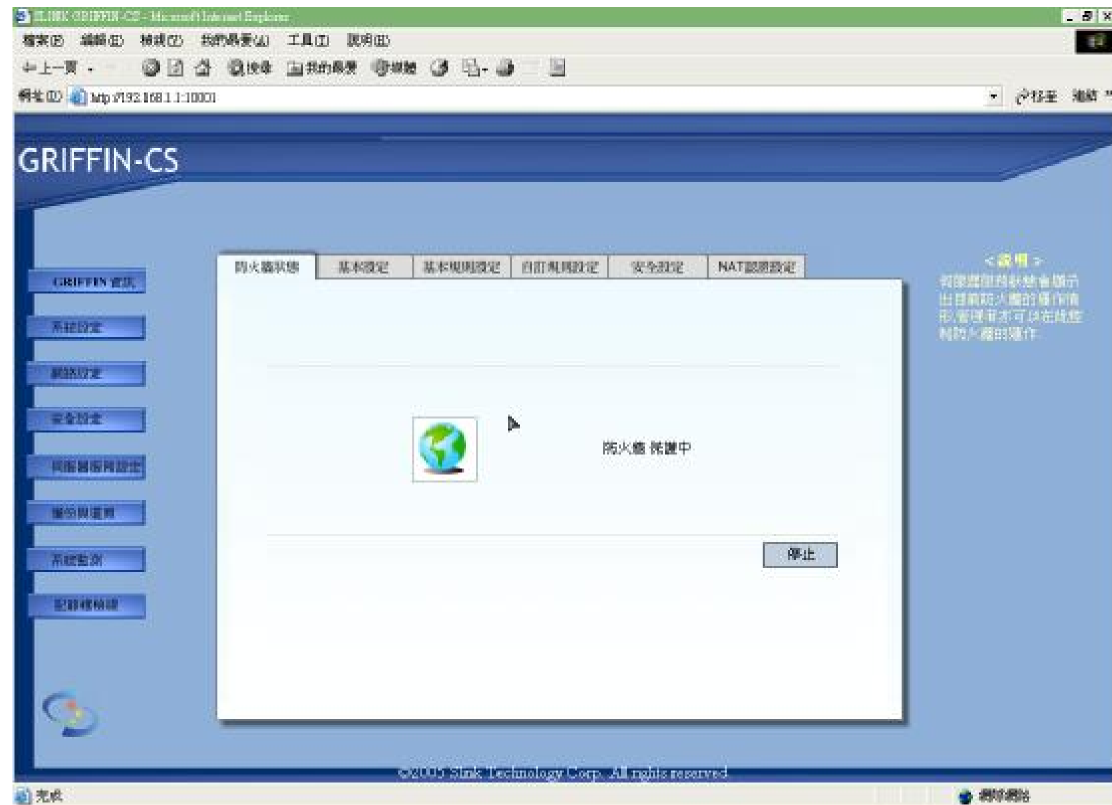
當 GRIFFIN-CS2 察覺到被網路掃描時，便會自動將對方網路位置加入網路黑名單中，當 GRIFFIN-CS2 本身的防火牆有啓動時，便會完全的將這個網路位置的所有網路行爲抵擋掉（如網頁瀏覽），一直到管理者將這個網路位置從網路黑名單中刪除才可以恢復所有的網路行爲。

防火牆設定

GRIFFIN-CS2 內建防火牆核心，提供主機在網路上的多一層保護，其提供 7 大功能，NAT、封包過濾、封包轉址、防駭機制及 NAT 認證，其共有六小項，分述如下

防火牆裝態

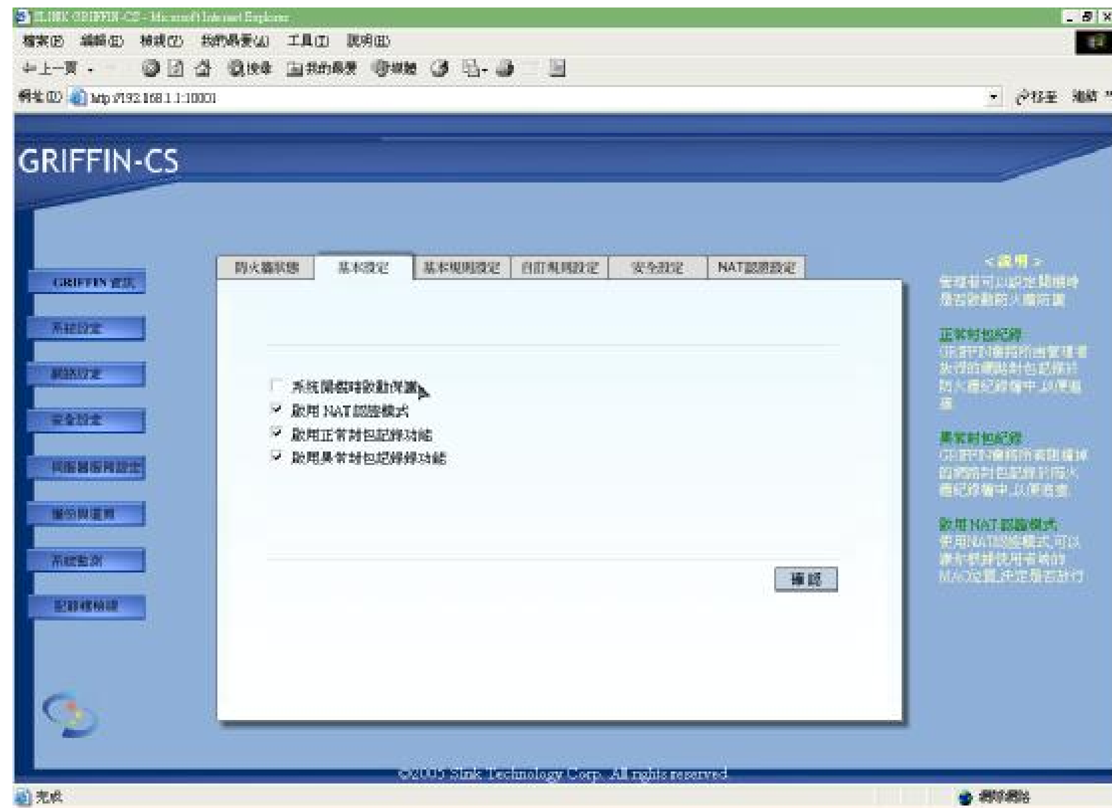
讓管理者可以監視這項防火牆的狀態，並在線上控制這項網路服務的是否運作，所以如果發現企業防火牆有問題，則第一時間就是先檢視這防火牆服務有無問題。



如果要企業內部要使用 GRIFFIN-CS2 的 NAT 功能，請確定防火牆在保護中，如此運作才正常。

基本設定

這裡讓管理者可以設定是否在 GRIFFIN-CS2 開機時自動啓動防火牆



啓用 NAT 認證模式

這個選項可以讓您管控在 NAT 環境下，使用者上網的情形，主要便是對個使用者電腦的 MAC 做管控，不在允許的使用者電腦，即使是位在企業內部 NAT 環境中，一樣無法上網存取，更詳細說明請參考 NAT 認證設定章節。

正常封包記錄功能

在基本規則及自訂規則設定的防火牆規則，只要是準許的服務埠號就屬於正常埠，當啓用這功能時，所有的經由準許的服務埠號網路連線，都將被記錄下來。

異常封包記錄功能

在基本規則及自訂規則設定的防火牆規則中，當啓用這功能時，所有不經由準許服務埠號的網路連線，都將被記錄下來。

注意

防火牆的記錄檔成長相當迅速，所以如果非常必要，建議可以不使用這兩個功能，增進防火牆效率。

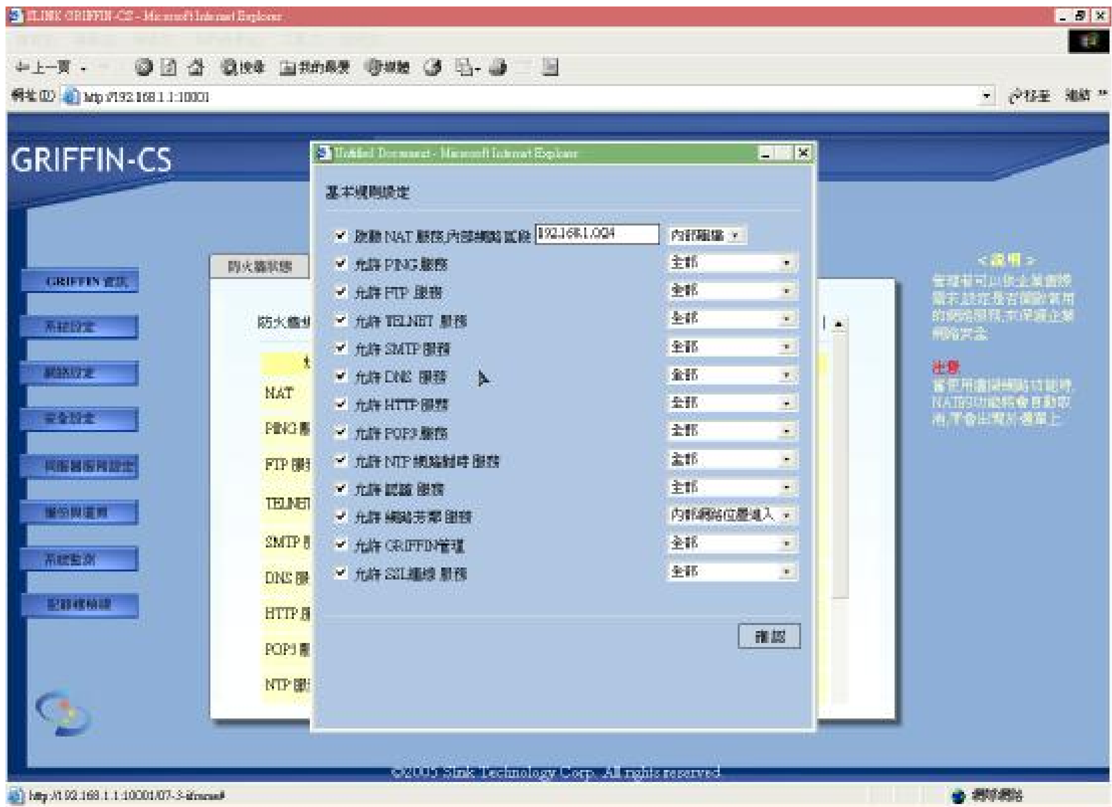
基本規則設定

基本規則設定會列出目前常用網路服務的封包過濾狀態，管理者可以輕易從圖中得到訊息，

	表示此網路服務是允許通過的
	表示網路服務是不允許通過的



管理者可以相當輕易的在此設定所要開啓的網路服務，按下設定後會出現如下畫面



管理者可依企業的需求的，勾選要開放或阻擋的網路服務，其內定網路服務說明如下

GRIFFIN-CS2 目前的防火牆連線範圍分爲下列

名稱	說明
外部	所有從外部網路介面進入的封包
封包通道	本封包傳輸通道
內部	所有從內部網路介面進入的封包

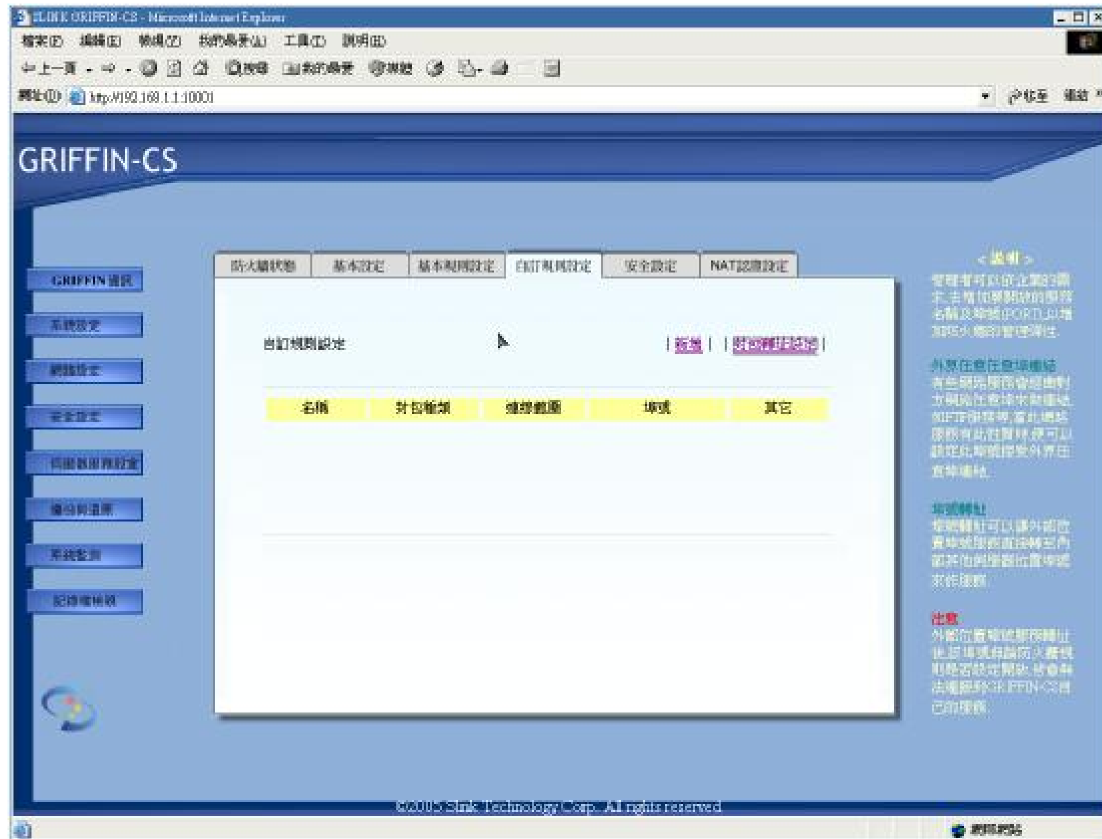
舉例說明

如果今天 GRIFFIN-CS2 負責公司的 NAT 及網頁服務，則當你設定允許 HTTP 服務的連線範圍爲外部時，則只有透過外部網路可以存取網頁服務，其公司內部電腦一概無法存取 GRIFFIN-CS2 的網路服務，而當設定爲封包通道時，則內部電腦可以存取外部的網頁服務，如上 YAHOO 網站，但是 GRIFFIN-CS2 無法存取，而當設定爲內部時，則僅有內部電腦可以存取 GRIFFIN-CS2 所以提供的網頁服務。

名 稱	說 明	埠 號
NAT	啓動 NAT 功能,讓內部網路可以連線到外面網路	--
PING	允許 PING,tracroute 來查看網路設備是否關閉服務	8
FTP DATA	允許 FTP 資料 檔案存取相關服務	20
FTP	允許 FTP 檔案存取相關服務	21
TELNET	允許 TELNET 相關服務	23
SMTP	允許 SMTP 寄信相關服務	25
DNS	允許 DNS 網路位置查詢相關服務	53
HTTP	允許 HTTP 網頁瀏覽相關服務	80
POP3	允許 POP3 網路收信相關服務	110
NTP	允許 NTP 網路時間校正服務	123
認 證	允許網路信件認證 相關服務，打開是讓一些使用該 113 確認身份的主機不至於反查時會卡住很久	113
網 路 芳 鄰 服 務	允許網路芳鄰服務	137-139
GRIFFIN 管 理	允許外部網路存取 GRIFFIN 管理介面	10001
SSL	允許 SSL 網頁服務	443

自定規則設定

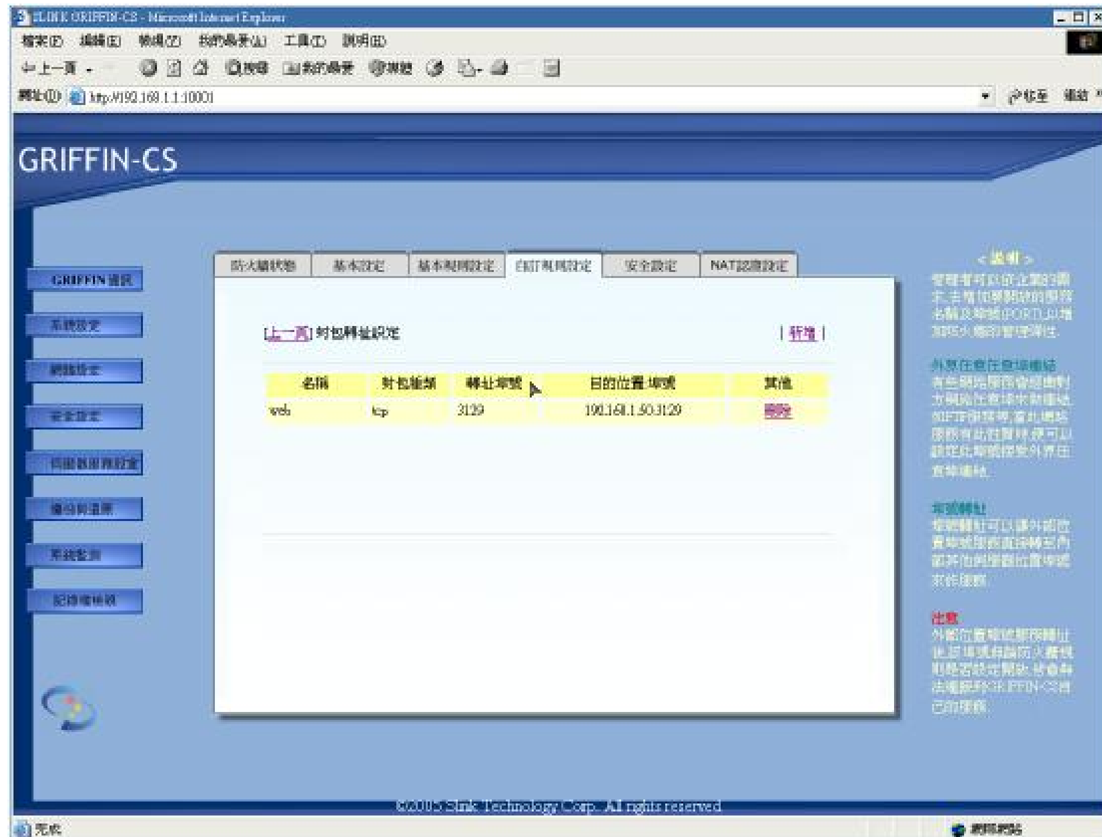
自定規則設定提供管理者，在基本規則不足的部分，能夠自行訂定一些網路服務，如 MSN、PC ANYWHERE 等



管理者設定時請輸入網路服務名稱，開放封包種類、連線範圍及埠號，及是否開放外部任意埠連結，及是否開放連線端 1024-65535 的連結，因爲有相當多的網路服務，其使用者端對其連線時，並不是透過相同的埠號連線，而是從 1024-65535 中任意開其一個埠號與該網路服務連線，所以如果有如此特性的網路服務，請必須勾取開放連線端 1024-65535 的連結。

封包轉址設定

封保轉址設定可以讓管理者輕易的將外部特定埠號的存取轉進入內部特定伺服器特定埠號，亦即所謂 PORT MAPPING 的功能。



舉例說明

如果企業已經有網頁伺服器了，也希望這網頁伺服器繼續服務，又希望 GRIFFIN-CS2 可以當作第一線的防火牆，則便可以在此設定，將外部 80（一般網頁伺服器的服務埠號）埠的存取，導到內部網頁伺服器網路位置的 80 埠上，請記得這台內部的網頁伺服器的網路閘道（GATEWAY）要指向 GRIFFIN-CS2 的內部網路位置，如此才能運作正常。

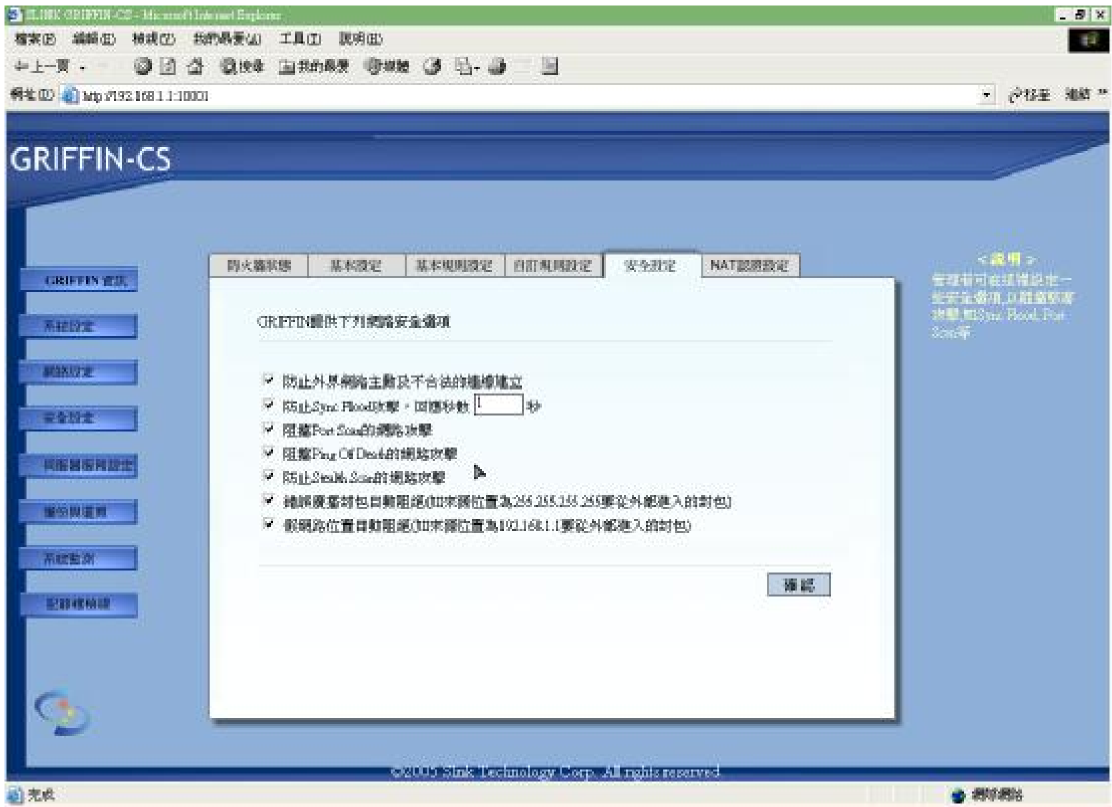
注意

當您在此設定了轉址埠號後，該埠號無論您 GRIFFIN-CS2 的防火牆設定如何，皆會以此網路轉址設定埠號設定為主。

如果您要在外部透過類似 PC ANYWHERE 軟體直接存取管理內部伺服器，則請在此設定，以確保可以存取正常。

安全設定

安全設定提供管理者一些防止駭客的基本功能，與入侵偵測配合更可以得到倍加的功效。



目前 GRIFFIN-CS2 提供四大選項，分別說明如下

- 防止外界網路主動及不合法的連線建立
  對於一些主動與 GRIFFIN-CS2 連線或網路位置不合法的封包，一律抵擋掉

- 防止 Sync Flood 攻擊
  Sync Flood 攻擊會對於要攻擊的系統發出一連串的 SYN 封包，每個封包會讓系統回應一個 SYN-ACK 的封包，然後系統會等待對方送出 ACK 封包，系統紀錄序列中的 SYN-ACK 封包，必須等到收到對方的 ACK 封包後或超過逾時時間後才會移除，如果同時間被大量的這種封包攻擊，最後系統會因爲充滿了 SYN-ACK 封包，而喪失網路功能。

- 阻擋 Port Scan 的網路攻擊
  可避免掉一些無謂的網路掃描，此爲將所有掃描封包丟棄，即掃描不到這台 GRIFFIN-CS2，進而放棄攻擊。

- 阻擋 Ping Of Death 的網路攻擊
  此攻擊手法爲利用 Ping 程式一直發送大於 65536 bytes 的 ping packet 到目標主機，產生超過 IP 協定所能准許的最大封包，讓被攻擊主機過於忙碌而當機

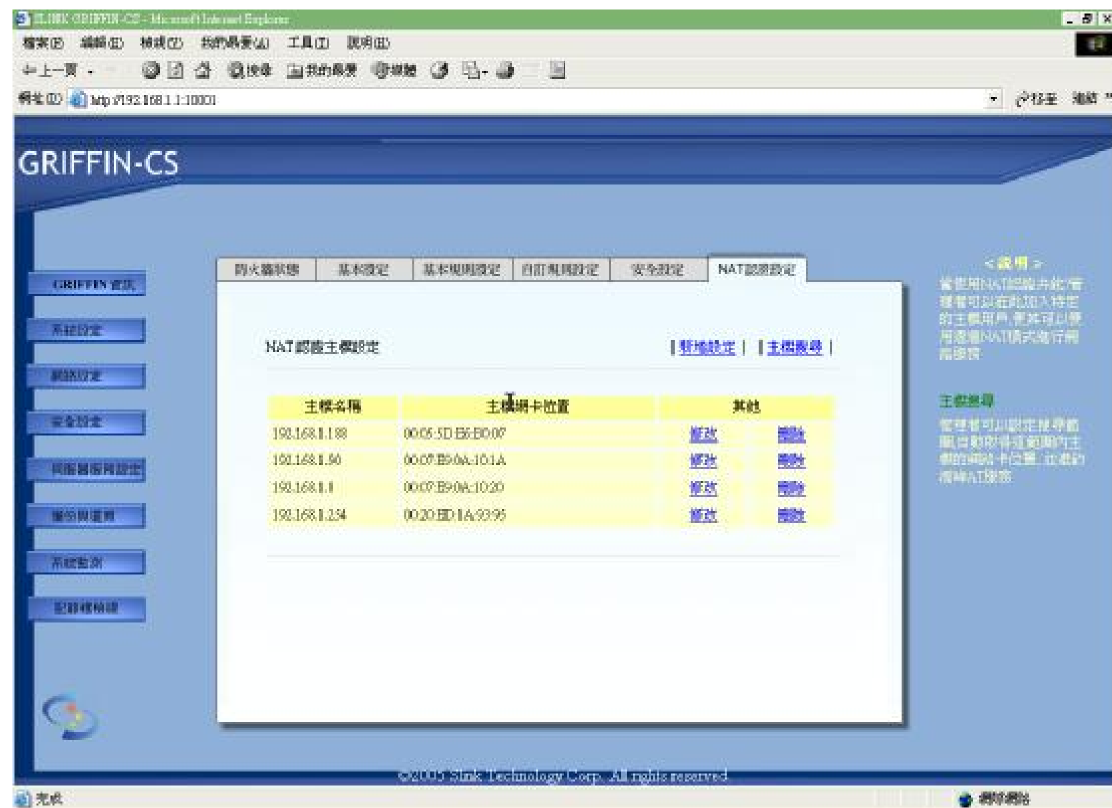
- 防止 Stealth Scan 的網路攻擊
  防止外部 TCP 隱形掃描的攻擊。

- 錯誤廣播封包自動阻絕
  如來源位置爲 255.255.255.255 要從外部進入的封包

- 假網路位置自動阻絕
  如來源位置爲 192.168.1.0/24、10.0.0.0/8、172.16.0.0/12、127.0.0.1、224.0.0.0/4、240.0.0.0/5 要從外部進入的封包

NAT 認證設定

當您在基本設定中，啓用 NAT（網路位置轉址）認證設定時，所有使用者電腦的 MAC 位置，如果不在 NAT 使用者列表中，便無法透過 GRIFFIN-CS2 上網做網路存取。



- **主機搜尋**

  可以自動找尋在一個網路區域內的所有使用電腦的 MAC 位置，透過這一功能，您便可以相當容易的找尋出 192.168.1.1-254 這個網路區域所有電腦的 MAC 位置，並且所有找尋到的使用者電腦 MAC 位置會自動加入允許上網清單內，而您可以視實際需求進行管控的動作。

伺服器服務設定

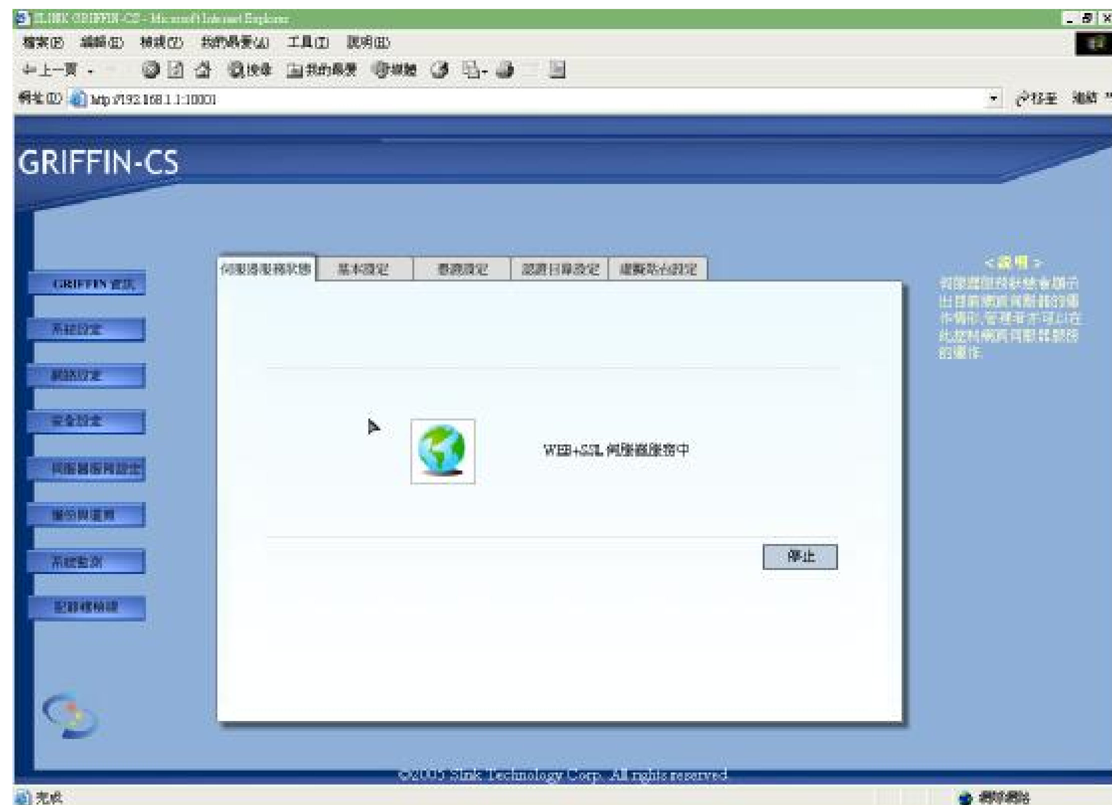
伺服器服務設定的功能讓管理者可以相當容易的管理這台機器的網路服務功能，目前 GRIFFIN-CS2 共含有 6 大網路服務功能，分述設定如下

WEB 設定

WEB 設定提供企業設定檢視目前網頁伺服器的功能，共有五小項，分述如下

伺服器狀態

讓管理者可以監視這項網路服務的狀態，並在線上控制這項網路服務的運作，所以如果發現企業網頁服務有問題，則第一時間就是先檢視這網路服務有無執行。



基本設定

這裡讓管理者可以設定是否在 GRIFFIN-CS2 開機時自動啓動這項服務



- **n** 個人網頁目錄

  當有使用這功能時便可以透過 http://your-domain/~帳號來做個人網頁檔案的存取，內定的索引檔爲 index.html。

- **n** WEBMAIL

  WEBMAIL 可以提供企業類似 YAHOO 網路郵件的功能。

- **n** 網路硬碟

  網路硬碟可以提供企業員工透過網頁來存取電腦檔案的功能，並可以讓企業自行訂定最大的上傳檔案大小，內定爲 5MB，此部分的數字最好視企業網路頻寬下去訂定，不然相當容易將企業網路頻寬耗盡。

- 啓動 SSL 支援

  當管理者完成憑證設定後，基本設定中變會出現本功能選項，當如果要網頁伺服器支援 SSL 傳輸的話，便需勾取此功能，如此便可以提供使用者以 https://localhost/ 的方式來存取企業網頁。

  如果 GRIFFIN-CS2 有使用防火牆的功能，則請記得勾取 SSL(443)支援。當您要勾取或取消本選項時，請先停止網頁服務

- 啓用虛擬網站支援

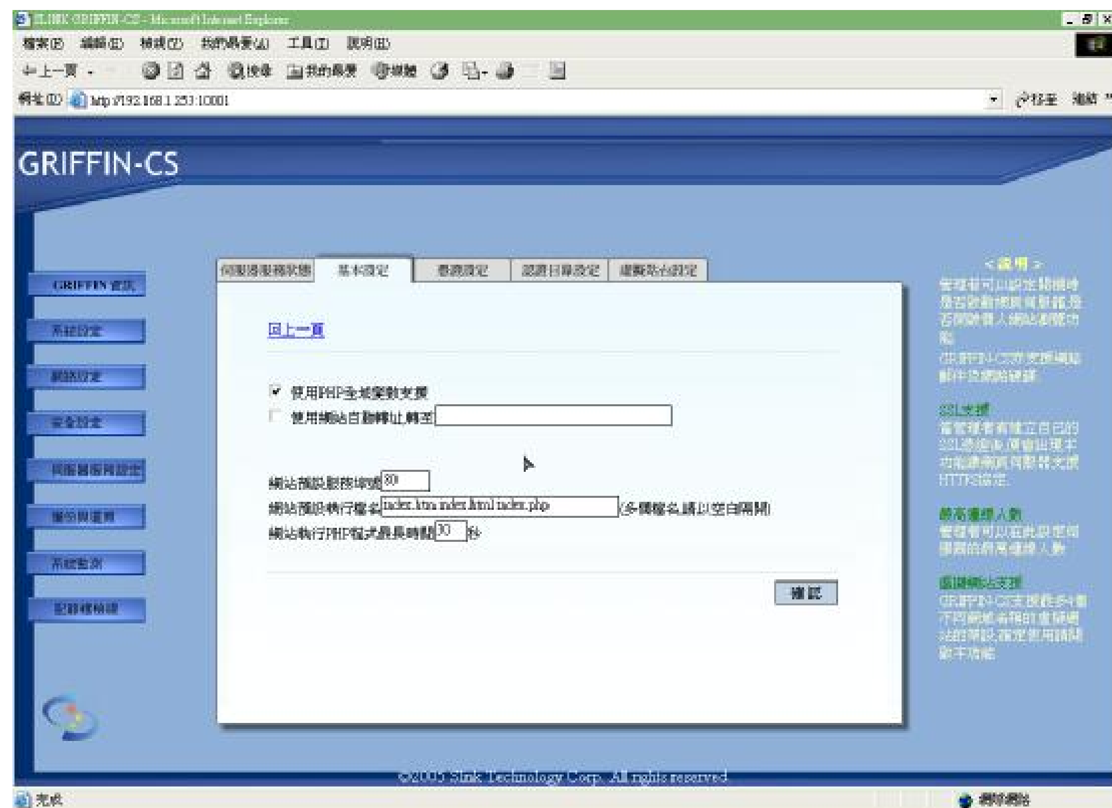
  GRIFFIN-CS2 目前最高可以支援 4 個虛擬網站，可以讓企業同時擁有 4 個不一樣網域名稱的網頁，如 www.test1.com.tw、www.test2.com.tw 等，詳細的設定方式請參後面的說明

- 最高連線人數

  GRIFFIN-CS2 可以讓企業自訂目前最高的通時連線人數，150 爲內定值，如果您 SERVER 的效能較佳，可以將此數值訂定高一點，以增加網頁伺服器的最大服務人數。

進階功能設定

按下進階設定後，會出現下面畫面



- 使用 PHP 全域變數支援

  此功能選項爲設定是否讓 PHP 支援全域變數，有些 PHP 開發的套裝軟體會要求你必須使用這功能，不然會造成程式無法正確執行

- 使用網站自動轉址

  此功能可以讓管理者設定是否將 GRIFFIN-CS2 首頁，轉換到某一個特別的網頁，比如說如果希望網站瀏覽者預設便透過 https 來做連線，便可以在此設定轉至 GRIFFIN-CS2 本身的 HTTPS 服務，如 https://your_domain/，當然此前提是你必須啓用 GRIFFIN-CS2 的 SSL 支援功能

- 網站預設服務埠號

  可以讓管理者自行變更網頁服務的埠號，目前內定爲世界通用的埠號 80。

- 網站預設執行檔名

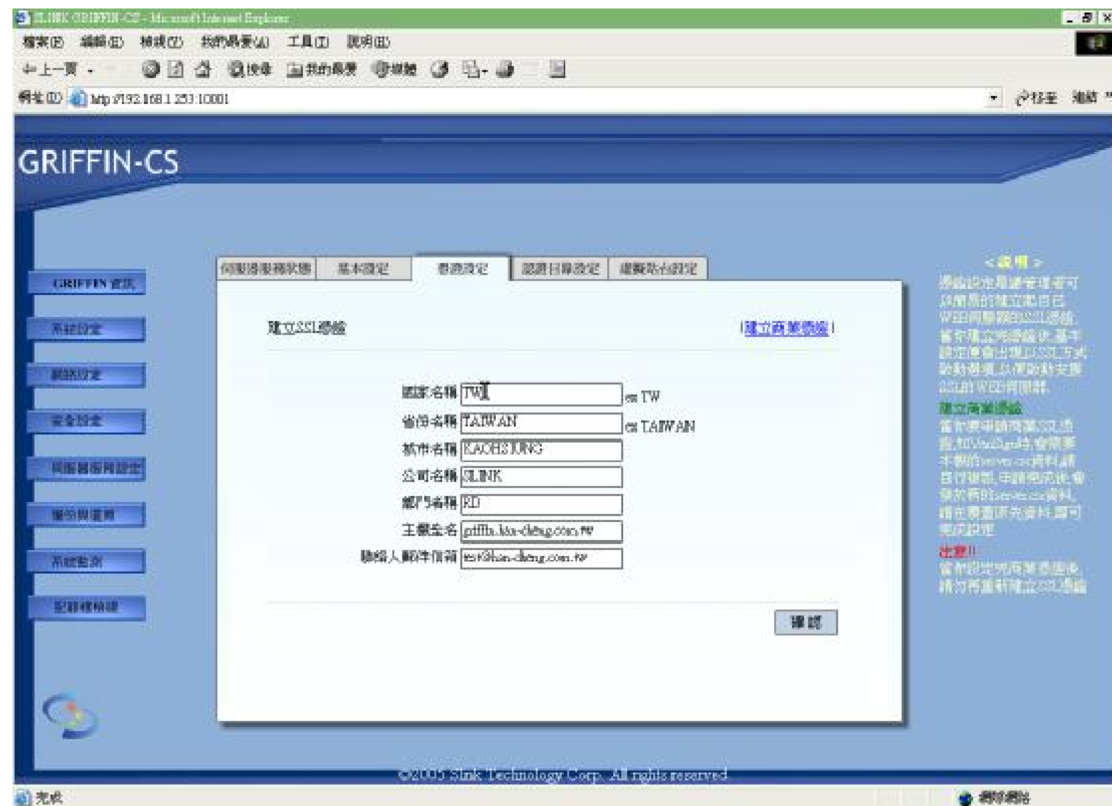
  可以讓管理者自行定義網站預定執行的網頁檔名，可以設定多個檔名，設定時需以空白隔開

- 網站執行 PHP 程式最長時間

  可以讓管理者控制 PHP 程式執行的時間，內定建議爲 30 秒。

憑證設定

此功能主要是讓管理者可以輕易的建立起企業的 128 位元的 SSL 網路安全憑證，進而可以使 GRIFFIN-CS2 提供 HTTPS 的安全性網頁服務



因為目前的憑證發放還是以國外為主，所以在此請勿鍵入中文資料，以免發生錯誤。

建立完憑證後，基本設定中會出現啓動 SSL 支援，勾起重新啓動 WEB 伺服器既可。

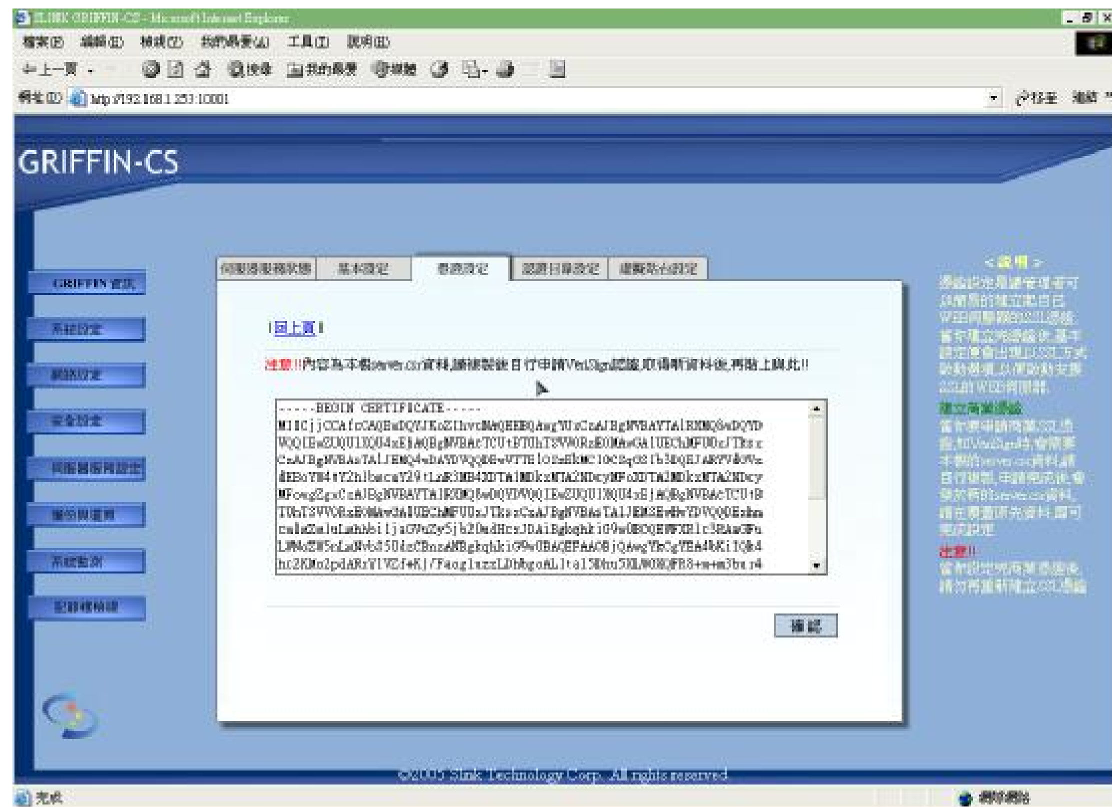
使用者端就可以用 https://you_name/瀏覽 GRIFFIN-CS 系列網頁資料內容。

注意

此憑證僅可以代表公司，但非為經由世界性認證中心所發的憑證，如 VeriSign 等，但它可以保證使用者端與企業的連線資料是加密過的，而非一般明碼。

建立商業憑證

如果希望網站所發放的憑證爲是世界認證的，如 VeriSign 等，便可以在此設定



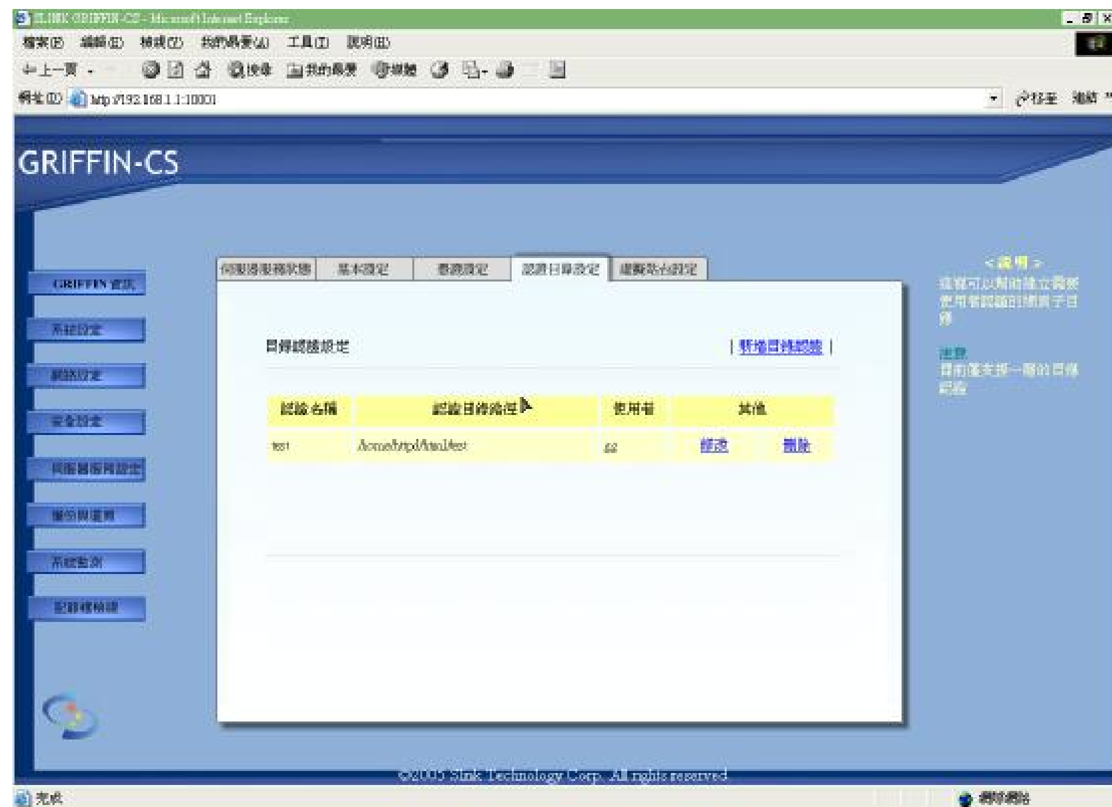
畫面上出現的爲目前 GRIFFIN-CS2 所產生的 SERVER.CSR 檔內容，當你申請商業用憑證時，便需要這個資料進行申請，申請完後商業憑證發放中心，會寄給新的 SERVER.CSR 給您，您便直接將新的資料直接覆蓋舊資料即可。

注意

當您已經安裝完成新的商業憑證後，請勿在重新建立新的 GRIFFFIN-CS 憑證，不然會造成你所安裝的商業憑證遭到覆蓋，並且需要重新變更申請資料，再重新申請一次，不然就必須在等候 14 天，以舊的申請資料，重新申請商憑證一次，並在安裝一次。

認證目錄設定

認證目錄設定可以讓企業快速建立需要認證的網頁資料，如重要的公司文件等，如此當網頁瀏覽者進入這個目錄時，便需要輸入認證使用者名稱及密碼。



注意

目前只支援根目錄下的一層目錄，系統會自動去抓取，所以在新增設定前，請先於根目錄下，新增你要保護的目錄，不然新增時，認證目錄名稱會出現空白。

虛擬站台設定

GRIFFIN-CS2 目前最高可以支援 4 個虛擬站台，要使用本功能，請先在基本設定中勾取啟用虛擬網站支援



系統會自動根據目前的網域及外部網路位置產生一筆資料，此為不可刪除的。

當您新增虛擬站台時，您需要指定一個本機使用者作為管理者，系統將自動於此本機使用者個人目錄中新增一個 www.new_domain 的目錄，此即為此虛擬網站的資料目錄。

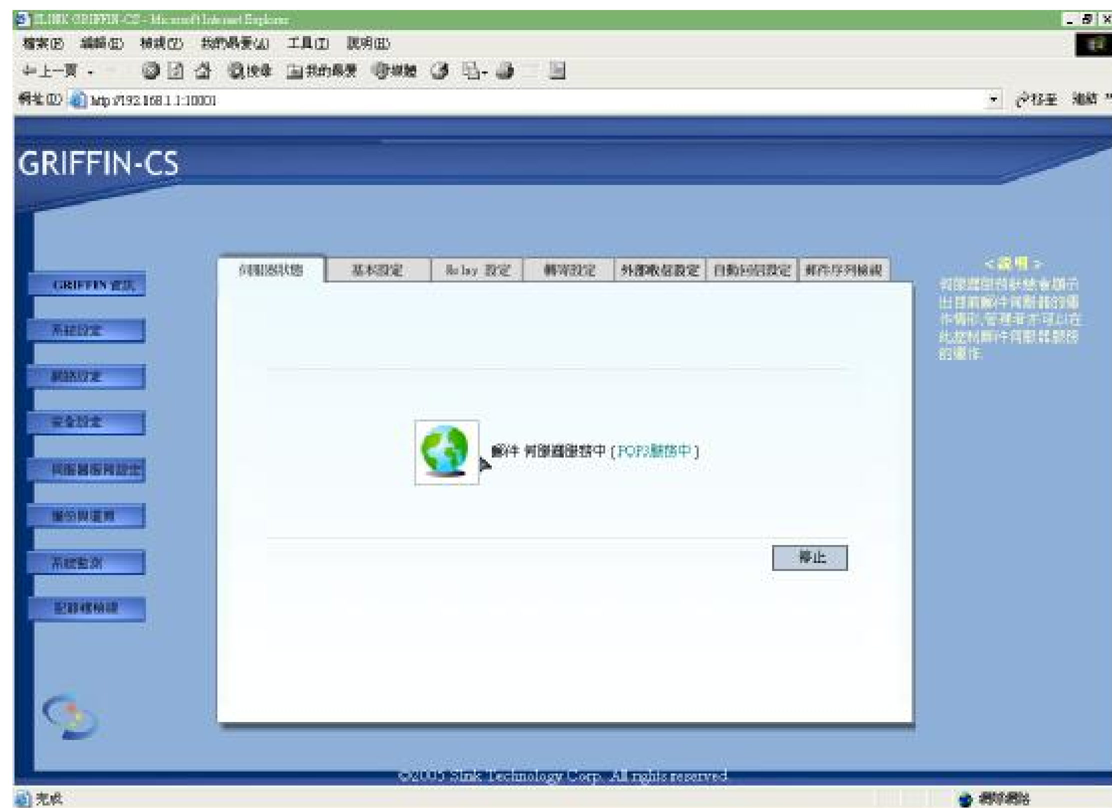
- **n** 自動設定 DNS
  當您新增時您可以勾取此選項，系統會自動幫你產生新的 DNS 網域對應資料，並自動幫您重新啟動 DNS。

MAIL 設定

MAIL 設定提供企業設定檢視目前郵件伺服器的功能，共有七小項，分述如下

伺服器狀態

讓管理者可以監視這項網路服務的狀態，並在線上控制這項網路服務的運作，所以如果發現企業郵件服務有問題，則第一時間就是先檢視這網路服務有無執行。



基本設定

這裡讓管理者可以設定是否在 GRIFFIN-CS2 開機時自動啓動郵件伺服器服務，是否啓用 SMTP 認證，是否啓動 POP3 服務、及設定傳送郵件大小。

如果企業要使用 outlook express 或 outlook 等使用者端的郵件收信服務，請務必勾取啓動 POP3 服務

如果企業要限制公司內部的收信的大小，如不想公司內部使用者外寄 mp3 等大型檔案，則可以在這邊做限制。

GRIFFIN-CS2 亦支援 SMTP 寄信認證服務及 POP-BEFORE-SMTP 的 POP3 認證功能，管理者可以擇一使用選擇啓動，可以使得企業員工可以在世界各地透過 GRIFFIN-CS2 來寄送郵件，而不用擔心員工在外或在家因郵件 RELAY 問題而無法寄信，讓企業寄信 anywhere。



- 外寄郵件認證

  GRIFFIN-CS2 亦支援 SMTP 寄信認證服務，當管理者啓動這項服務，則下次要寄信時便需要輸入使用者名稱及密碼，啓動此功能，可以使得企業員工可以在世界各地透過 GRIFFIN-CS2 來寄送郵件，而不用擔心員工在外或在家因郵件 RELAY 問題而無法寄信，讓企業寄信 anywhere。

- 啓動網路黑名單阻隔

  GRIFFIN-CS2 支援網路黑比對阻絕功能，當使用這功能時，郵件在收信時會去 dsn.rfc-ignorant.org、relays.ordb.org 做比對，如果對方是在黑名單中便自動拒絕收取信件。

- 忽略郵件帳號大小寫

  如果您希望您的郵件伺服器收件時不區分收件者的大小寫，請勾取本選項。

- 使用網路範圍

  設定郵件伺服器的准許寄信網路範圍,網路設定精靈設定完成後會自動設定一個值，如企業設定的爲網路位置爲 192.168.1.2，GRIFFIN-CS2 會自動設定爲 192.168.1.0/24 這個區段，如果企業有其他的區域要加入，直接修改即可，加入時請記得以”, “逗號加一空白隔開不同網路區段。

- 設定報表分析範圍

  GRIFFIN-CS2 提供三種郵件報表供管理者檢視，管理者可在此設定報表的分析時間範圍，可以設定爲今日、昨日、本週、本月。

- 郵寄郵件報表

  GRIFFIN-CS2 提供郵寄 2 種分析報表的功能，分別說明如下

  郵件分析統計表

  管理者可以相當簡易的透過郵件來了解各分析時間範圍的郵件處理情況可以設定爲今日、昨日、本週、本月。

  郵件即時記錄報表

  管理可以相當簡易的透過此郵件報表來了解目前郵件所收送的情形,何封信發生錯誤，何種錯誤。

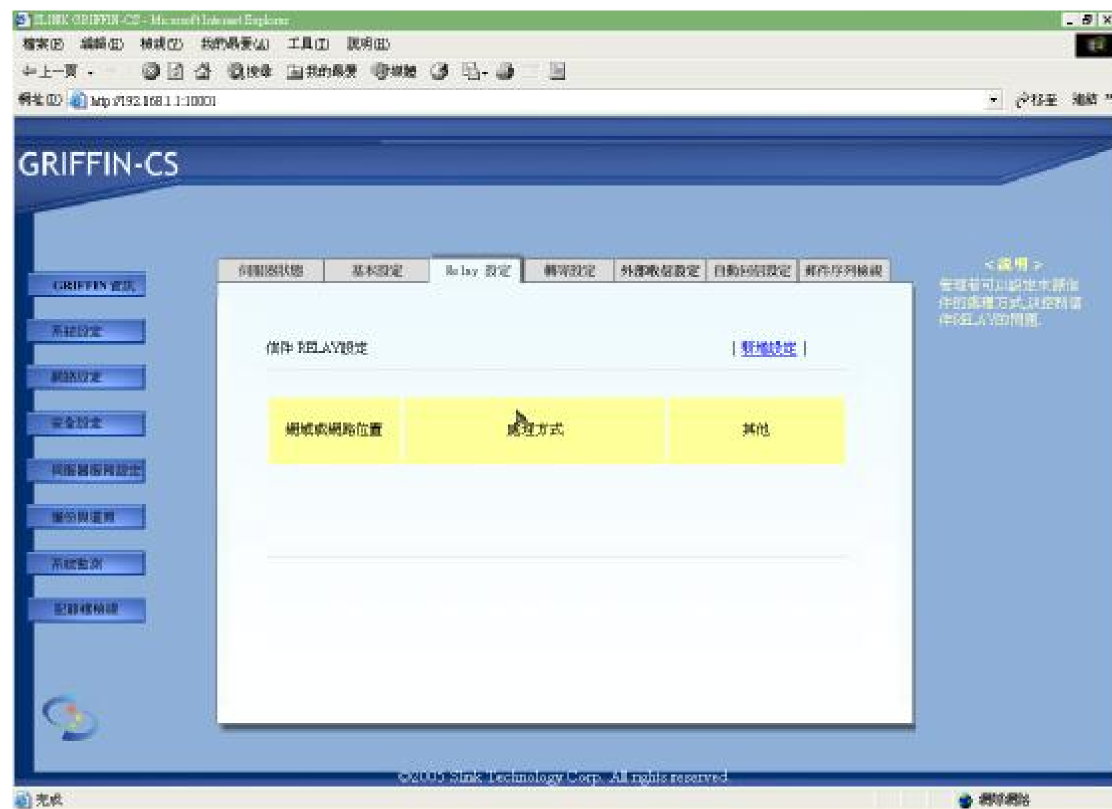
- 收信網域設定

  GRIFFIN-CS2 目前提供最大 4 個不同網域的收信功能，就是說一間企業最高可以支援到 4 個不一樣的網域來收信，假設公司有申請兩個網域，test.com 及 test.com.tw，則 test 這個使用者可以收到寄到 test@test.com 及 test@test.com.tw 的信件

設定完成後請按確認完成設定。

Relay 設定

面對目前網路上廣告郵件 RELAY 問題氾濫，GRIFFIN-CS2 亦可以提供企業避免成爲郵件 RELAY 的對象，GRIFFIN-CS2 的郵件伺服器，內定的只可以 RELAY 本機，所以當管理者要設定內部網路電腦，將這 GRIFFIN-CS2 設爲內定郵件伺服器時，請記的將內部的網路設定爲允許 RELAY，不然內部網路會變成無法寄信。



特別說明

原則上這一部份可以忽略設定，因爲 POSTFIX 本身允許的 RELAY 位置，就是基本設定中的**使用網路範圍**

郵件或網路位置的設定範例如下

Yahoo.com	表示任何從 yahoo.com 寄送過來的信件
192.168.1	表示任何從 192.168.1.1-192.168.1.254 寄送過來的信件
test@test.com	表示任何從 test@test.com 寄送過來的信件

內定有三種處理方式，說明如下

接受 RELAY	從這個網址寄送過來郵件，可以接受，而且可以充當這個網址的郵件 RELAY 伺服器，建議只要設定內部網路即可
拒絕 RELAY	拒絕從這個網址寄送過來的郵件。
忽略	忽略這個網址寄送過來的信件，不做任何處理回應

所以針對一般公司而言，基本設定為【企業網域】及【企業內部網路位置】設定為接受 RELAY 即可。

1. 當啓用 SMTP 認證功能後，基本上就可以不用設定 RELAY。

如果管理者有啓用使用者認證服務（基本設定中），則此可以設定為*.*，拒絕 RELAY，所有的寄信動作皆須做使用者認證，才准許寄信動作。

轉寄設定

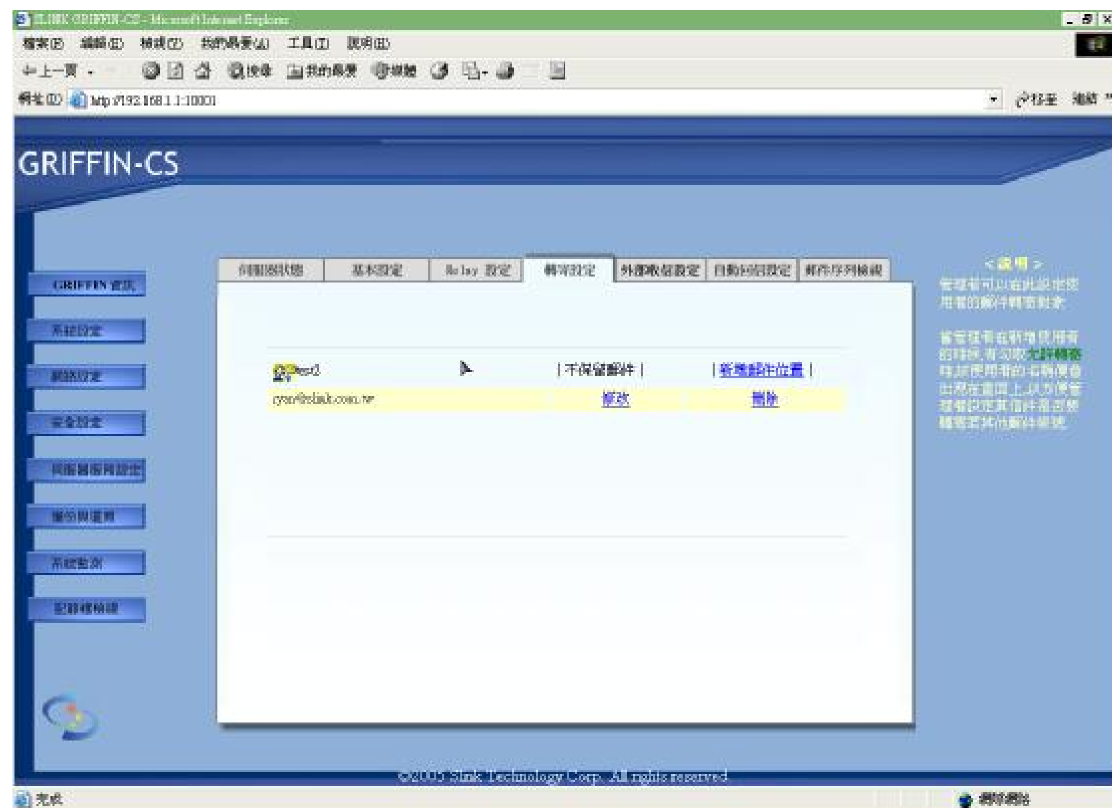
這裡可以讓管理者設定企業自訂的郵件寄件群組，但須與使用者管理配合，及假設企業的網域為 test.com，而希望建立一個 info@test.com 郵件轉寄群組，則請一下步驟

1.請先在使用者管理新增一個 info 的使用者，並在郵件轉寄部分設定為允許。

2.切換到這裡則管理者會看到 info 這個使用者，請在旁邊點選新增郵件位置。

3.此時會跳出一個小視窗，請輸入所要轉寄的郵件位置，按下確定即可。

4.管理者便會發現在 info 使用者下方會出現剛剛所設定的轉寄的郵件位置。

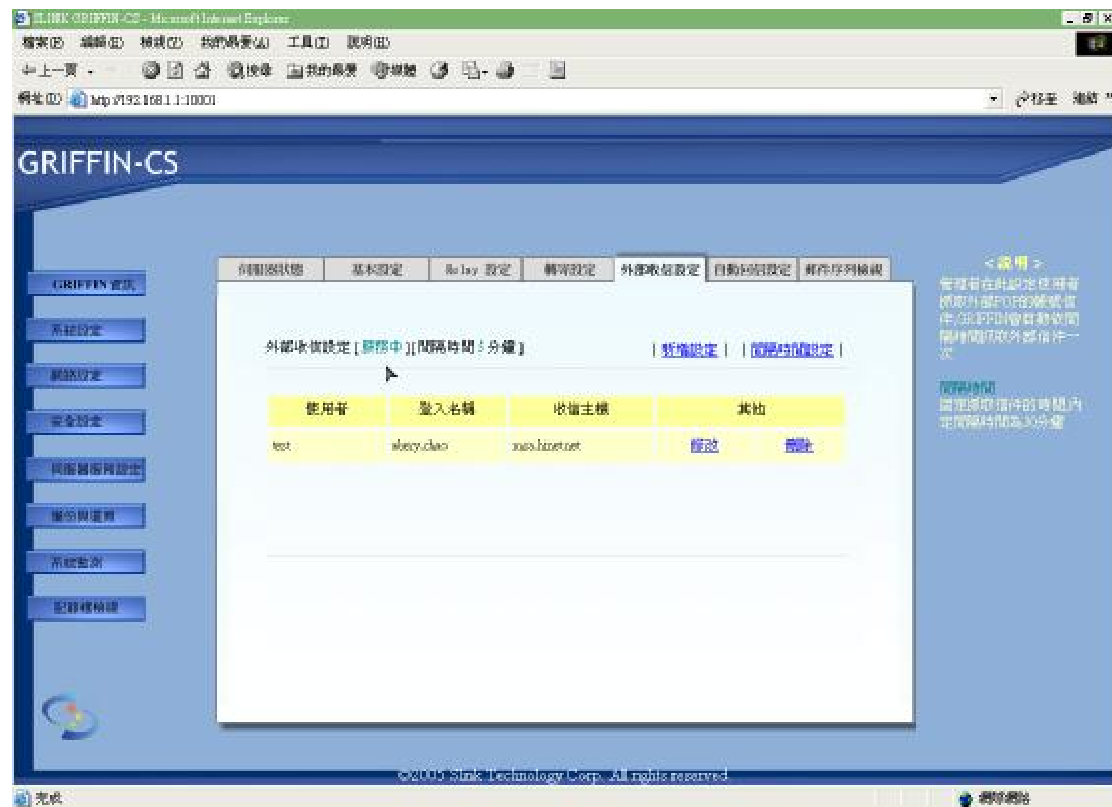


n 應用

企業可以先建立各種代表公司形象的名字，如 info、service、sales 等，然後啓動郵件轉寄，在此將郵件轉寄給相關人員。

外部收信設定

GRIFFIN-CS2 可以讓本機用戶，透過 POP3 協定收取外部伺服器的信件，如中華電信的信箱郵件等



- **n** 間隔時間

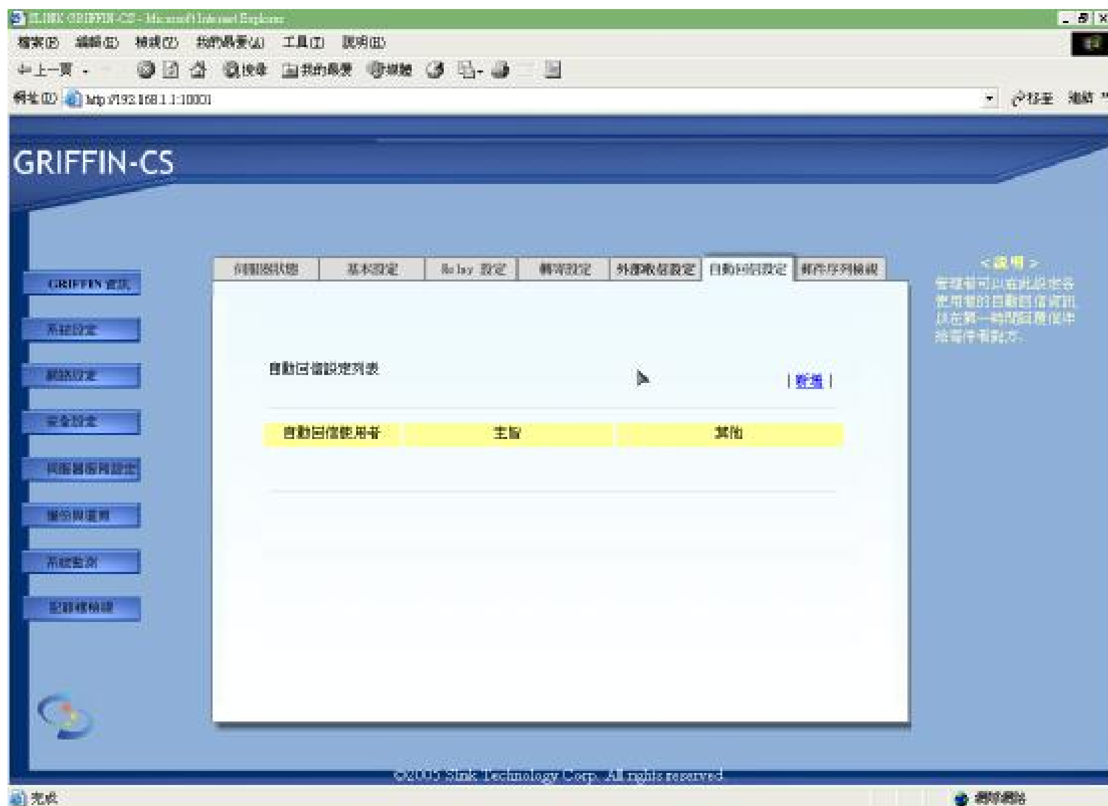
  GRIFFIN-CS2 可以讓你自行設定外部收取信件的收取時間間隔。

注意

當您有使用郵件掃描功能時，外部收取進來的信件，也會先被過濾。

自動回信設定

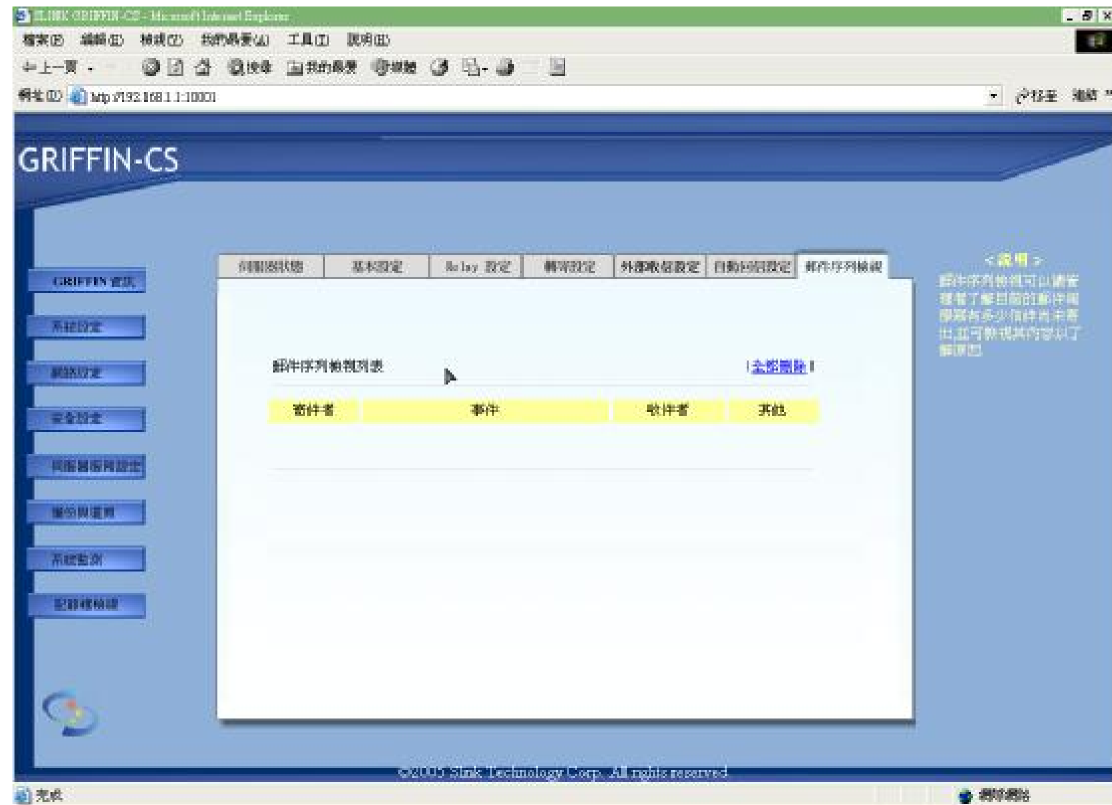
GRIFFIN-CS2 也提供了自動回信的功能，亦即如果企業有使用者有事休假或有段時間無法收看信，則管理者便可以在此設定自動回信，如此當有人寄信到管理者所設定的這個郵件位置時，便會收到管理者所設定的自動回信的內容。



此功能和轉寄設定結合可以完成自動回信轉寄系統，如企業可以設定一個對外業務郵件 salse@test.com，然後先設定轉寄給相關業務人員，再來設自動回信，如此如果有顧客對貴企業的商品有興趣，寄信給 salse@test.com 時，此時顧客便會立即收到一封感謝信，而相關人員也可以會收到這信件，並做處理，對公司企業的形像會大大的提昇。

郵件序列檢視

郵件序列檢視提供管理者去檢視目前郵件伺服器的寄信情形，是否有太多的信件在序列中等待寄送。



一般而言管理者可以透過這個功能來檢查 GRIFFIN-CS2 是否有太多的信件等待寄送，是何種信件一直未能寄送，是否因公司郵件 RELAY 未設定完成，已經變成郵件 RELAY 站台，都可以透過這個功能來做檢視。

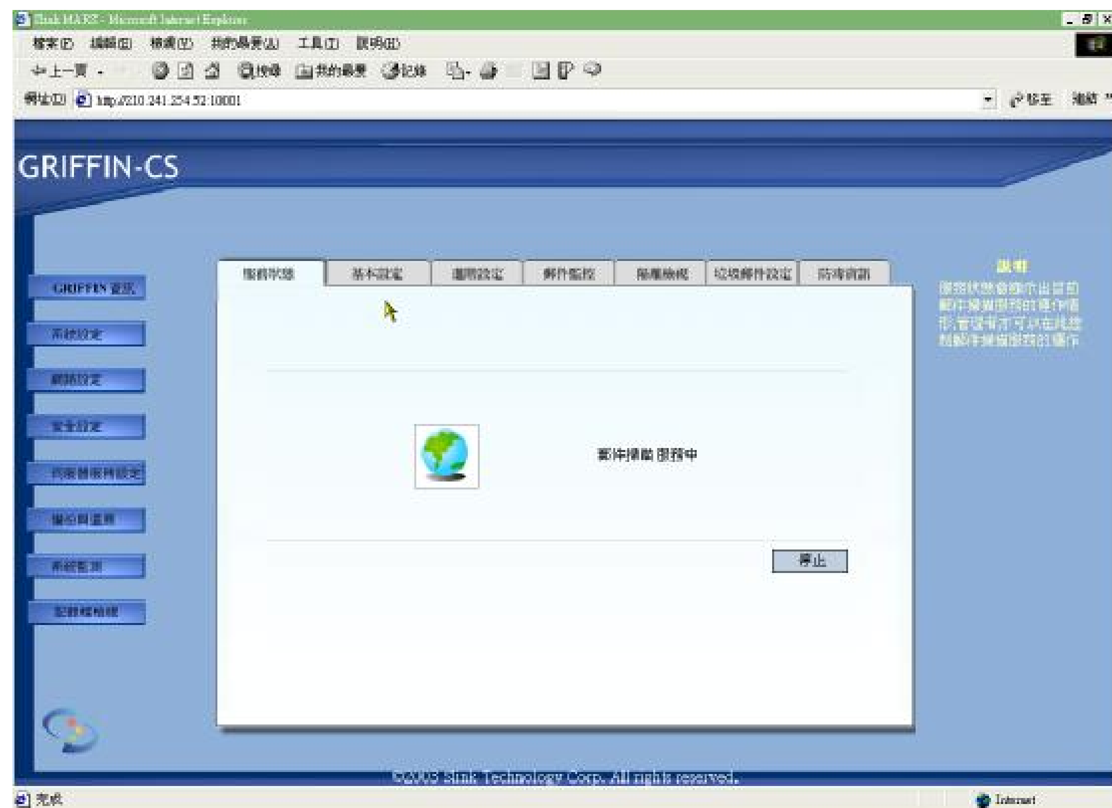
一般如果企業的郵件伺服器被當成 RELAY 站時，就會有相當多的郵件在序列等待。

MAIL 掃描設定

MAIL 掃描設定提供您企業設定檢視目前郵件掃描的功能（會與 MAIL 伺服器結合），共有七小項，分述如下

服務狀態

讓您可以監視這項網路服務的狀態，並在線上控制這項網路服務的是否運作，所以如果發現企業郵件服務有問題，並且您有使用郵件掃描服務，則第一時間就是先檢視這網路服務有無問題。

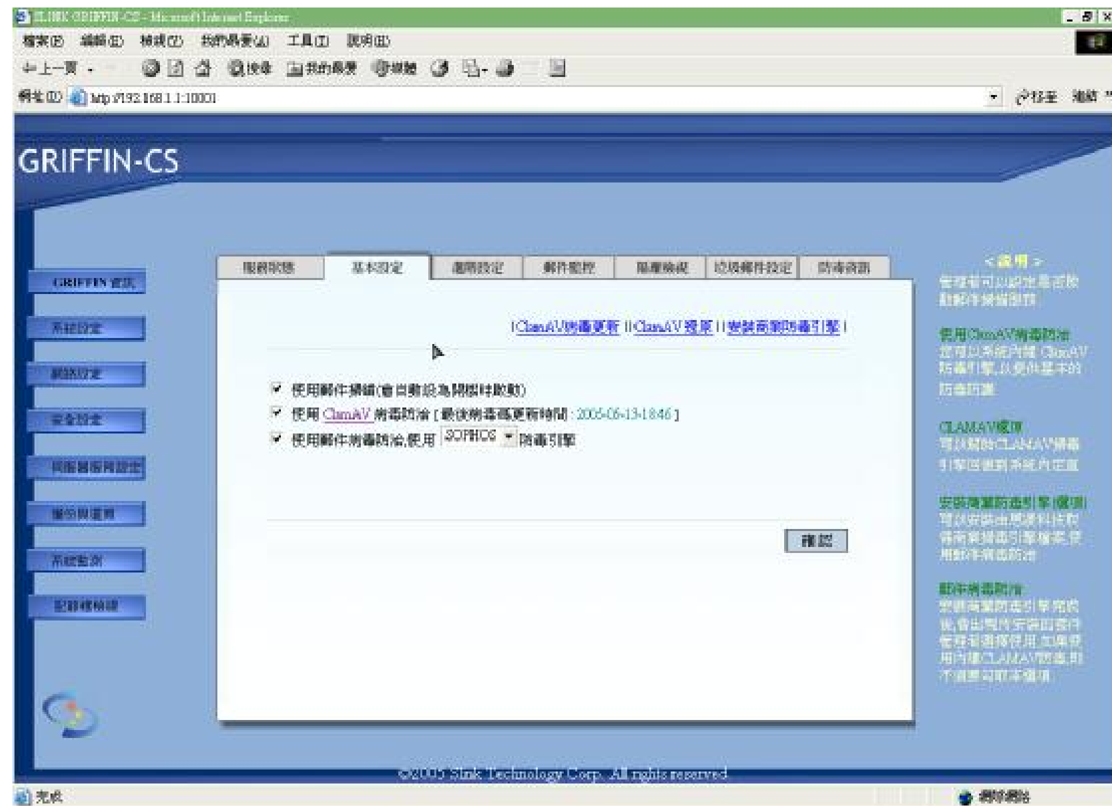


注意!!

當您沒有在基本設定中勾取使用郵件掃描服務時，不會出現本畫面，而是出現一個要求您先勾取使用郵件掃描服務的頁面，請先至基本設定中勾取設定後，即可正常控制這項網路服務。

基本設定

這裡讓您可以設定是否在 GRIFFIN-CS2 開機時自動啓動這項服務



GRIFFIN-CS2 目前可以支援郵件閘道掃毒的功能，就是當信件進入您郵件伺服器時，會先經過一道掃毒的程序，先在第一時間確認收取的信件有無病毒，目前 GRIFFIN-CS2 內建 CLAMAV（www.clamav.net）這套免費的掃毒引擎，直接勾選就可以使用，當您勾選使用後，GRIFFIN-CS2 就會每日自動的至 CLAMAV 網站更新病毒碼。

- **CLAMAV 病毒更新**

  讓您馬上更新系統病毒碼（第一次更新病毒碼會需要數分鐘的時間，請耐心等候）

- **CLAMAV 還原**

  可以幫助您還原系統 CLAMAV 掃毒引擎至最初狀態

除了免費的 CLAMAV 外，GRIFFIN-CS2 亦可以支援 SOPHOS（www.sophos.com）這家英國全球防毒公司的掃毒引擎技術。

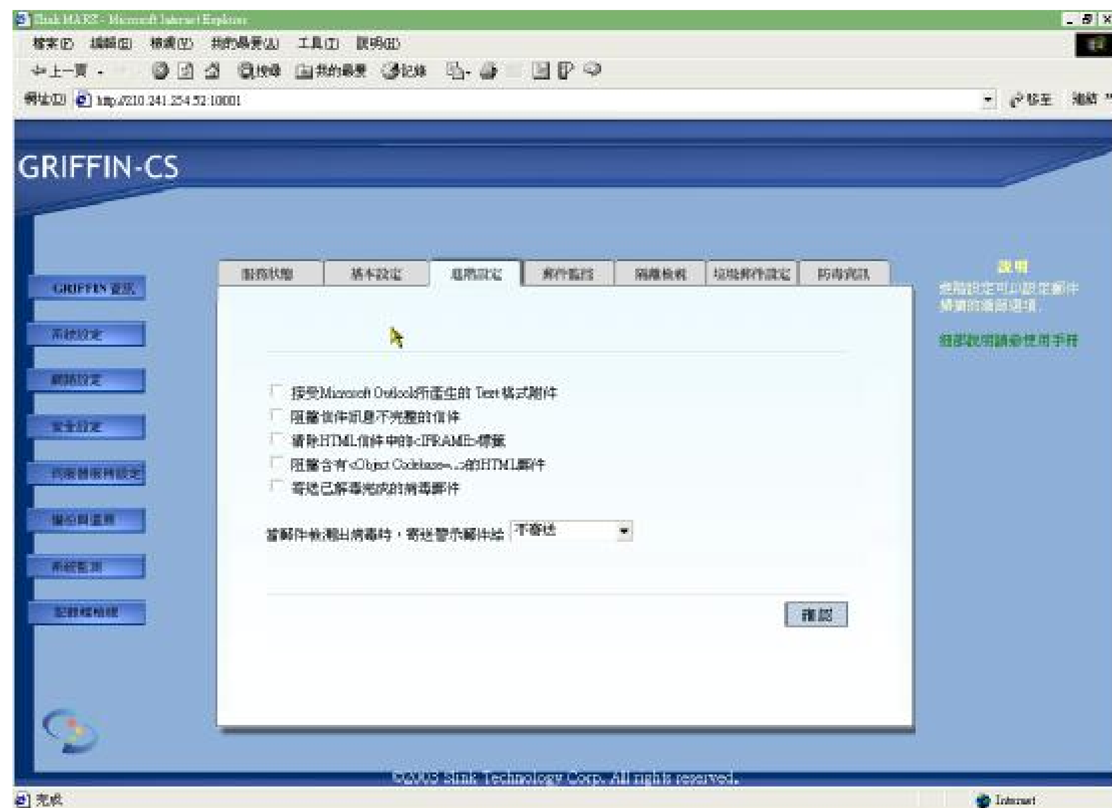
這技術需要另外付費購買，當您已經取得需要付費的程式 linux.intel.slink.tgz 之後，如何安裝呢？相當簡單，請先確定 SAMBA 網路服務有啓動，透過網路芳鄰進入 GRIFFIN-CS2 伺服器中，進入 PUBLIC 這個目錄中，建立一個 SOPHOS 的目錄，再將 linux.intel.slink.tgz 這個檔案複製到此目錄中，然後執行安裝方毒引擎就會出現 SOPHOS 這個選項，按下確定即會自動安裝完成。

此時你便可以勾取使用病毒防治，會自動出現 SOPHOS 防毒引擎供您選擇。

您亦可以同時勾選兩套防毒引擎做爲防護，不過如此會耗費相當的系統資源，這點請管理者自行評估再做決定。

進階設定

這裡讓您可以設定 MAIL 掃描時的一些進階選項



- 接受 Microsoft Outlook 所產生的 Text 格式附件

  一些 Microsoft Outlook 版本會產生擁有很多 Text 格式的附件，這些附件目前並不能被完全的解譯，您如果是使用大量的 Microsoft Outlook 的用戶，請勾取此選項。

- 阻擋信件訊息不完整的信件

  不完整的訊息當然不能被掃出有病毒，就如同每次處理都只有片段的資訊，不得有完整的訊息，不勾選這個選項是『非常危險』的事，因爲假設病毒存在不完整的訊息中，將無法被察覺。

- 清除 HTML 信件中的<IFRAME>標籤

  清除 HTML 信件格式中，含有<IFRAME>這個標籤，一般來說有可能會直接呼叫另一個網頁，而造成病毒入侵或導致被植入木馬。

- 阻擋含有<Object Codebase=...>的 HTML 郵件

  清除 HTML 信件格式中，含有<Object Codebase>這個標籤，一般來說有可能會直接呼叫有害的系統元件，而造成病毒入侵或導致被植入木馬。

郵件監控

GRIFFIN-CS2 提供郵件秘錄的功能，亦即管理者可以設定一個監控管理者帳號，並設定要監控的使用者，當被監控的使用者在做寄信或收信動作時，系統就會自動複製一份到監控管理者帳號中，而對被監控的使用者來說是沒有任何異常的。



- 寄信監控
  使用者所有寄至外部的信件會被複製一份到監控管理者帳號
- 收信監控
  使用者所有收取的信件會被複製一份到監控管理者帳號
- 全面監控
  使用者所有寄至外部的信件及所有收取的信件會被複製一份到監控管理者帳號

注意!!

需先設定監控管理者，才會出現監控設定畫面，設定監控管理者及使用者帳號時，請輸入完整的帳號名稱，如 test@test.com.tw。

隔離檢視

這裡讓您可以檢視及設定被隔離異常郵件的大小及可以自行設定特定的檔案附件格式處理



- **n** 使用 SAMBA 隔離目錄分享(請記得重新啟動 SAMBA 服務)
  當你勾取這個選項後，請記重新啟動 SAMBA 服務，當您再度存取 GRIFFIN-CS2 網路芳鄰時，便會出現一個叫 mail_quarantine_dir 的目錄，這個目錄便是你儲存所有被隔離檔案的目錄，您可以利用信件編號找尋隔離的檔案。

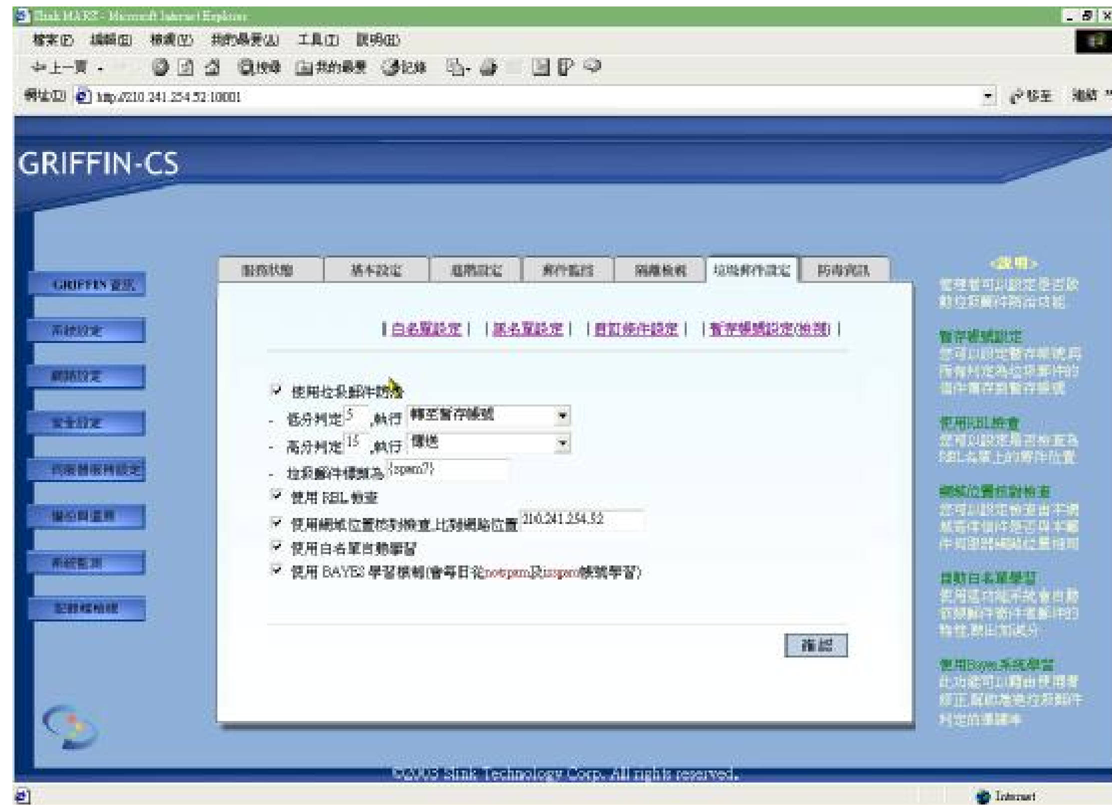
n 郵件檔案設定

可以讓您設定何種郵件檔案附件檔名要隔離，何種要放行，一般來說如果附件檔名爲*.pid，都是病毒居多，在此便可以做隔離的動作。



垃圾郵件設定

GRIFFIN-CS2 支援閘道端垃圾郵件防治的功能，其採用了 SPAMASSASSIN 的核心技術，以分數的加權來為每封信件評定一個分數，如果超過就判定為垃圾郵件，反之則為否，其並可以透過學習的機制，來增加信件判斷的準確率。



- **n** 低分判定

  這為第一程度垃圾郵件的分數設定，分數範圍為 1-15 分，內定為 5 分，一般的垃圾郵件皆會超過這個分數，可以視公司真實導入情形，來作調整，其共內定有五種的處理方式，傳送、轉寄至暫存帳號、刪除、刪除並通知寄件者、暫存並通知收件者，其中暫存帳號帳號的功能，需先執行暫存帳號設定，其選項才會出現。

  一般建議在此可以設定為轉寄至暫存帳號，如此如果有發生誤判的狀況，還可以到暫存帳號作檢視，找尋出誤判的信件，並轉寄給收件者。

- 高分判定

  這為第二程度垃圾郵件的分數設定，分數範圍為 10-25 分，內定為 15 分，超過這個分數幾乎有 99%為垃圾郵件，在此可以視公司真實導入情形，來作調整，其共內定有五種的處理方式，傳送、轉寄至暫存帳號、刪除、刪除並通知寄件者、暫存並通知收件者，其中暫存帳號帳號的功能，需先執行暫存帳號設定，其選項才會出現。

- 郵件標頭

  當您使用垃圾郵件防治的功能時，其 GRIFFIN-CS2 便會開始判定信件是否為垃圾郵件，如果為垃圾郵件時，便會在其信件標頭加註垃圾郵件標頭，內定為{spam?}，您可以採此自行作變更修改加註的文字。

- 使用 RBL 檢查

  當您使用這一個功能，GRIFFIN-CS2 便會開始利用 RBL 上的資料作分數的加權計算，如果信件寄件者是位在 RBL 名單上的，便會作加分的動作，使其成為判定為垃圾郵件。

- 使用網域位置核對檢查

  此一功能便是針對寄信網域名稱與郵件主機的網路位置作核對、檢查，以避免寄件者為您網域，其卻不是您企業的郵件主機所送出，在此比對網路位置請輸入您（郵件伺服器）GRIFFIN-CS2 的網路位置。

- 使用白名單自動學習

  當您使用此一功能時，GRIFFIN-CS2 便會自動的針對其寄件者來源作分析，如當一個寄件者或網路位置，常常寄送正常郵件的信件給你，系統便會自動記錄，以後這使用者或來源的信件自動作加權減分，避免誤判為垃圾郵件。

- 使用 BAYES 學習機制

  當您使用此功能後，GRIFFIN-CS2 會自動建立 isspam 及 notspam 兩個帳號，作為分析專用，如使用者收到的信件為正常信件，卻誤判為垃圾郵件，者可以請使用者將此信件轉寄到 notspam@your-domain 這個帳號，如果使用者收到的信件為垃圾郵件，卻沒有被判定為垃圾郵件，則可以請使用者將此信件轉寄到 isspam@your-domain 這個帳號，GRIFFIN-CS2 會自動每天作分析，並加入分數判定加權條件。

  此功能需要每個帳號已累積最少 200 封信以上開始有作用。

- 忽略中文標題字元檢查(中文國家適用)

  因為中文字碼為兩個字元組成，勾取此功能會忽略的中文字元檢查，減少中文誤判機率。

- 白名單設定

  管理者可以將一些確定爲正常寄信者郵件位置加入白名單內,以避免誤判發生。

- 黑名單設定

  管理者可以將一些確定爲異常寄信者郵件位置加入黑名單內,直接判定爲垃圾郵件。

- 自訂條件設定

  管理者可以自行訂定一些特別字串，如”色情’、”sex”等字串，給予一個加權分數，增加判斷的準確度

- 暫存帳號設定

  可以讓管理者設定暫存帳號，設定完成後會出現轉寄到暫存帳號的選項，所有的垃圾郵件將會先寄至暫存帳號，如果有發生誤判時，便可以透過檢視去找出誤判信件，並將其轉寄到正確收件者上。

  要用檢視功能時,請先確定您 WEB 設定/基本設定/網路郵件功能有使用。

防毒資訊

當你有安裝商業性的防毒套件時，如 SOPHOS，防毒資訊讓您可以直接檢視目前掃毒引擎版本狀態



- **病毒碼更新**
  讓您可以立即線上更新病毒碼，直接去 SOPHOS 網站取得最新的病毒碼。

- **引擎更新**
  讓您可以立即線上更新病毒引擎，直接去思凌科技網站取得最新的病毒碼。

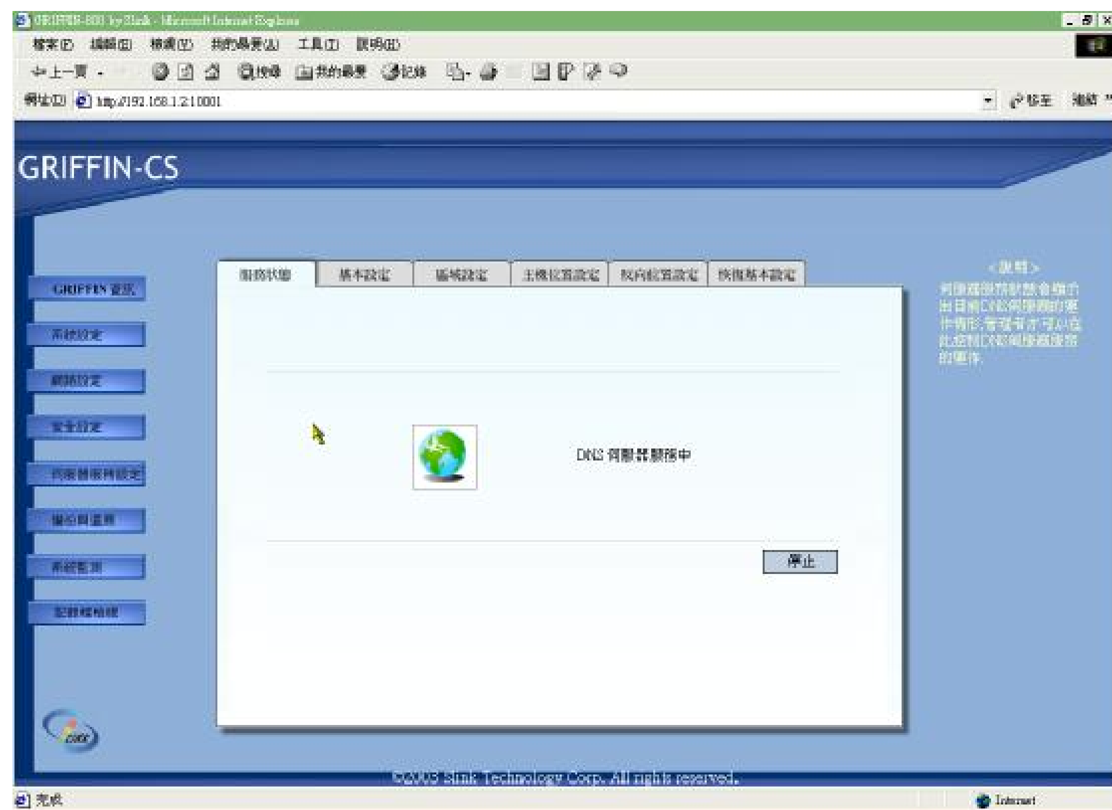
- **設定更新密碼**
  當您購買了 SOPHOS 的防毒授權後，思凌科技會給於您一組使用者名稱及密碼，當您設定完成後，便會出現每月掃毒引擎自動更新的選項，讓您可以自動到思凌的網站取得最新的掃毒引擎。
  請注意購買授權的日期，如授權已經過期可能會導致無法更新或更新失敗的狀況。

DNS 設定

DNS 設定提供企業設定檢視目前 DNS 伺服器（名稱解析伺服器）的功能，共有六小項，分述如下

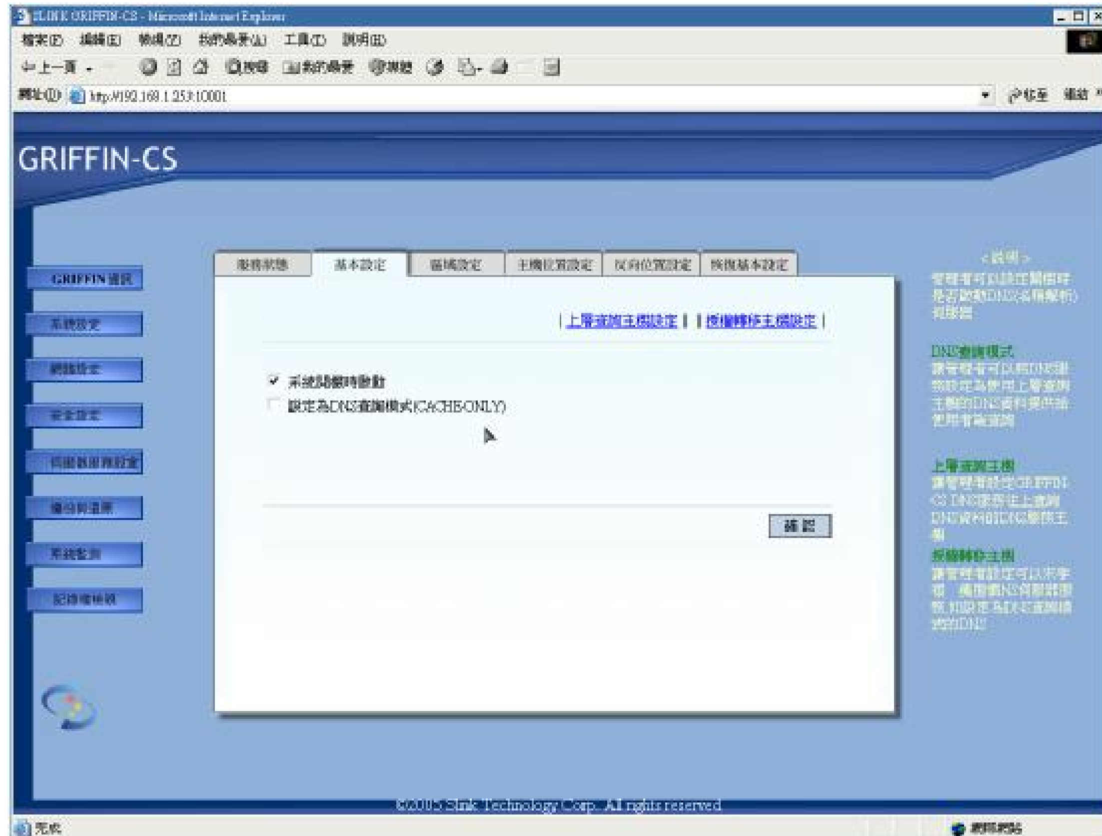
伺服器狀態

讓管理者可以監視這項網路服務的狀態，並在線上控制這項網路服務的運作，所以如果發現企業 DNS 服務有問題，則第一時間就是先檢視這網路服務有無執行。



基本設定

這裡讓管理者可以設定是否在 GRIFFIN-CS2 開機時自動啓動這項服務



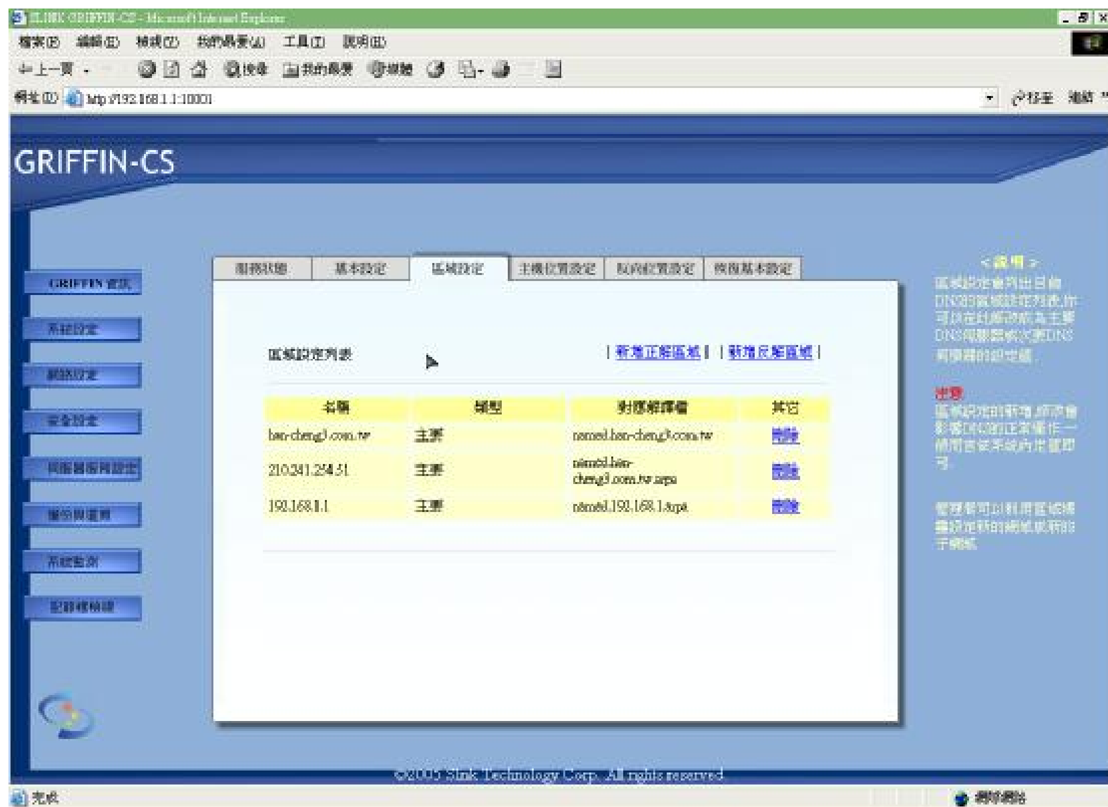
- **n** DHCP 查詢模式
  DHCP 查詢模式就是將 GRIFFIN-CS2 設定爲單純的只做查詢用的 DNS 服務，本身不做 DNS 管理，所有的 DNS 資料會從上層 DNS 取得，本身不提供 DNS 資料。

- **n** 上層查詢主機
  上層查詢主機就是 GRIFFIN-CS2 DNS 服務資料取得的 DNS 服務主機，如中華電信的 168.95.1.1 就是可以提供 DNS 資料取得的 DNS 伺服器。

- **n** 授權轉移主機
  GRIFFIN-CS2 本身可以當作上層查詢主機，內定是不允許下層主機取得 DNS 資料，如果您要開放，可以在此加入下層 DNS 網路位置，准許取得 GRIFFIN-CS2 DNS 資料。

區域設定

區域設定提供管理者增加相關對應的區域增加，GRIFFIN-CS2 在完成網路設定後，會依企業的網域完成三個內定值，分別為網域正解區域，外部網路位置反解區域及內部網路位置反解區域，此三個檔案皆可刪除，如果企業要將 DNS 設定為 SLAVE，則可以直接將此三個檔案刪除，設定新的 Slave 檔，將對應的的主要 DNS 主機輸入就可以了，目前 DNS 並無法支援密碼認證。



- **n** 新增正解區域

  輸入對應的網域名稱，即會自動產生對應檔。

- **n** 新增反解區域

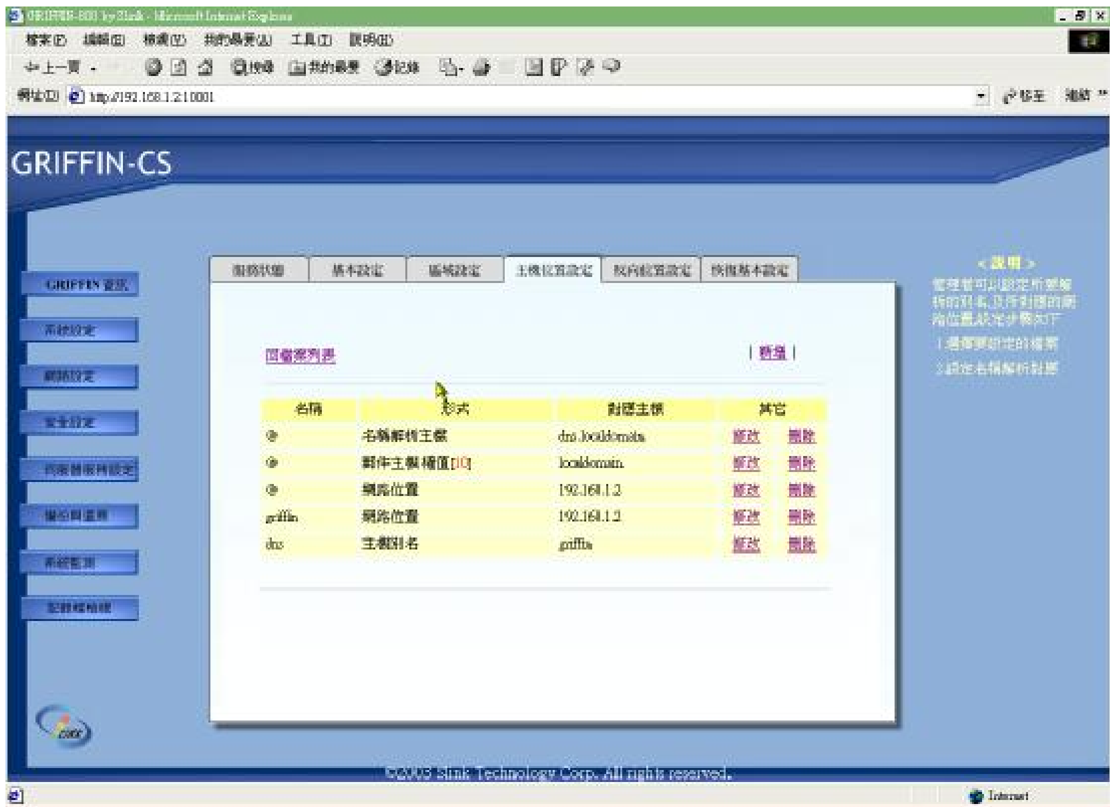
  輸入反解網路位置及對應的網域名稱，如 210.241.254.51 及 test.com.tw，就可以自動幫你產生對應檔，你可以選擇直接由網路位置作檔名（會產生 named.210.241.254.arpa）， 或者可以選擇自動選擇從網域名稱產生（會產生 named.test.com.tw.arpa）。

主機位置設定

主機位置設定讓管理者可以為企業網路增設專屬的網路名稱對應，畫面會先顯示出可以設定的所有區域設定的檔案，選擇完成後，按下一步，會顯示被選擇的對應檔的內容



而對應的方式分成四種，以名稱解析主機、郵件主機、實際網路位置，及依主機別名



名稱解析主機的意義就是指定將本網域的網路名稱解析交由對應的主機處理，一般採用系統內定值即可。

郵件主機即是指定寄來這個網域的郵件要由哪台郵件主機處理，其優先權值愈小，其優先權越高，就是寄來這個網域的信件會轉由優先權值愈小的主機處理。

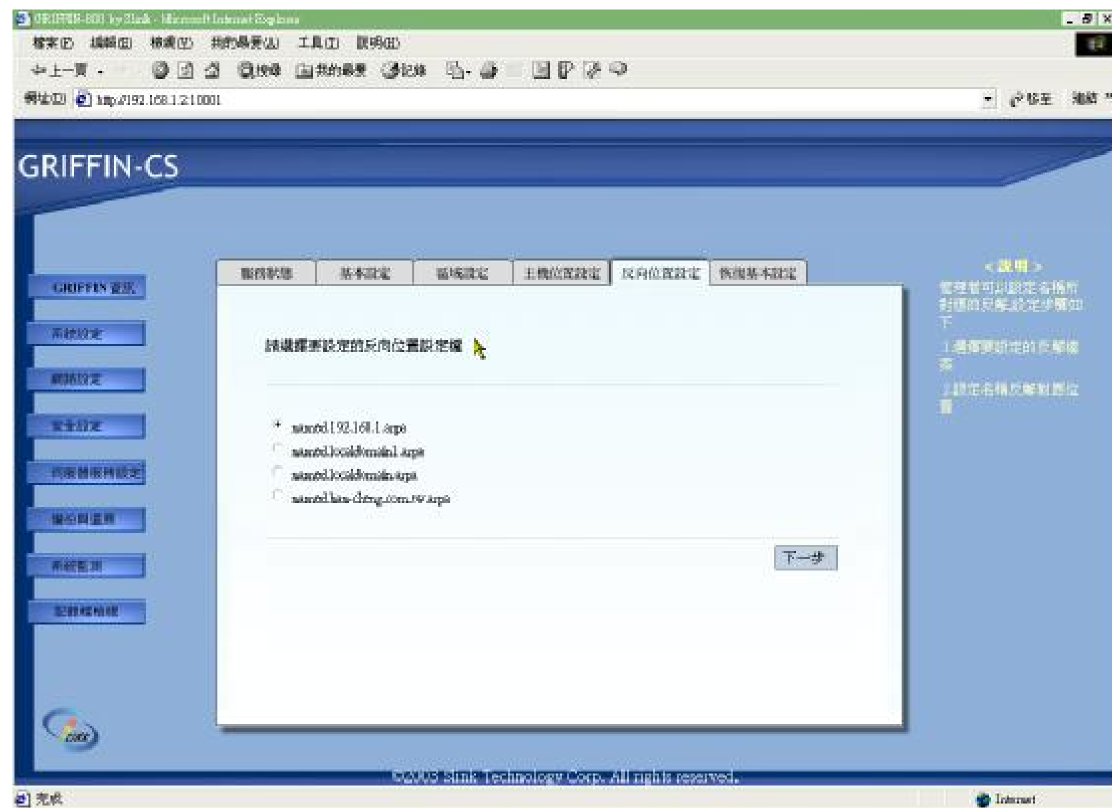
網路位置就是將實際的網路位置來提供 GRIFFIN-CS2 做網路名稱解析對應，如公司新增一電腦主機為 news，網路位置為 192.168.1.5，企業如果要提供外界查詢到 news.test.com，新增一網路位置對應，服務或主機名稱輸入 news，對應網路位置輸入 192.168.1.5 就可以。

主機別名的方式將會自動搜尋已經設定的網路位置解析設定，讓管理者選擇，GRIFFIN-CS2 在開始時便會一本身的網路位置產生主機別名設定，如果管理者要新增的主機解析設定爲 GRIFFIN-CS2，則可以使用內定的對應之別名。

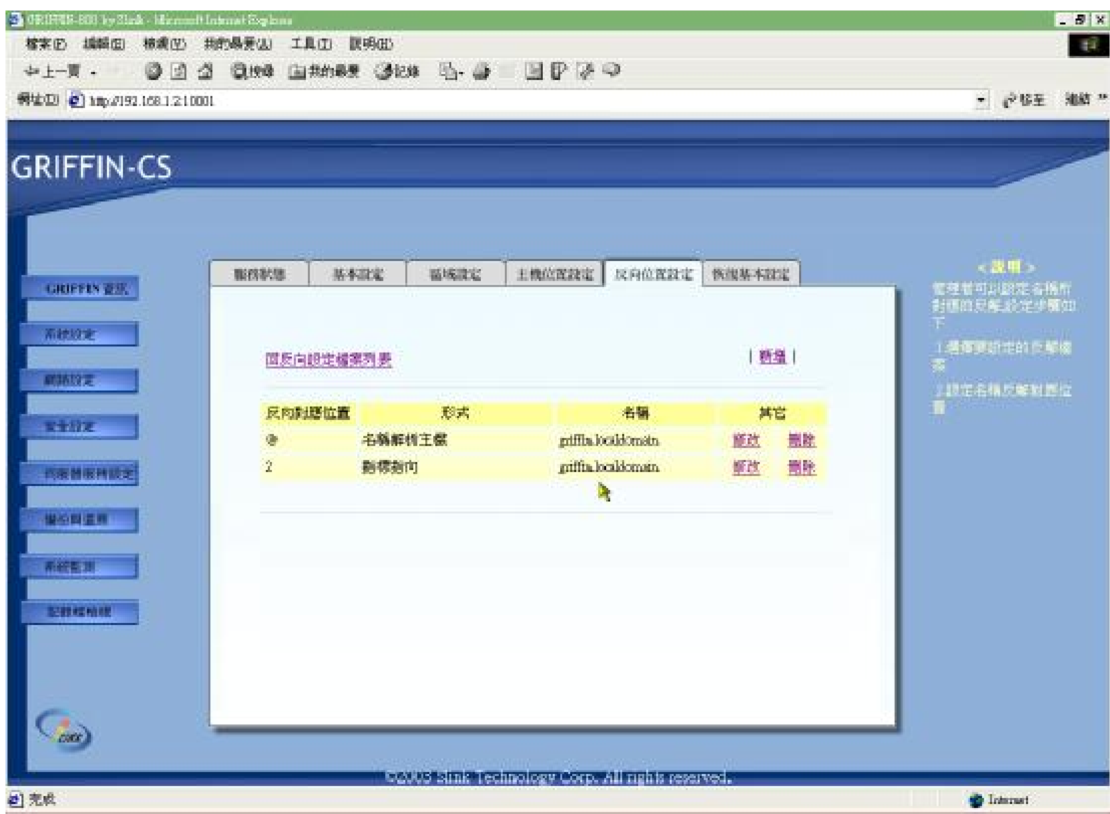
當管理者完成網路精靈設定後,內定的主機位置設定則會將 MAIL 位置及 DNS 位置指向 GRIFFIN-CS2，如果企業要外界主機也可以查詢到 www.your-domain.com，ftp.your-domain.com，則請新增主機位置設定，選擇主機別名的方式，將這兩的服務指向 GRIFFIN-CS2，則外界網路便可以鍵入 www.your-domain.com 找到 GRIFFIN-CS2 所以提供的網頁服務。

反向位置設定

反向位置設定讓管理者可以為企業網路增設專屬的網路名稱反解對應，畫面會先顯示出可以設定的所有反向設定的檔案（已.arpa 結尾的檔案），選擇完成後，按下一步，會顯示被選擇的反向對應檔的內容



而對應的方式分成兩種，以名稱解析主機、指標指向



名稱解析主機的意義就是指定將本網域的網路名稱解析交由對應的主機處理，一般採用系統內定值即可。

指標指向方式則爲最常用的方式，如企業如果在主機位置設定中新增了一個 new 的新網路位置對應爲 192.168.1.100，則在反向位置設定則需設定爲 100，指標指向形式，名稱則爲 new，如此一來網路上的任何一台機器，便可以知道 192.168.1.100，就是對應到 new 這個名稱。

回復基本設定

這裡將會按照目前的網路精靈設定，產生最基本的名稱解析設定檔，不過請注意，它將會將企業先前的主機位置設定資料刪除，所以本功能請相當小心使用。

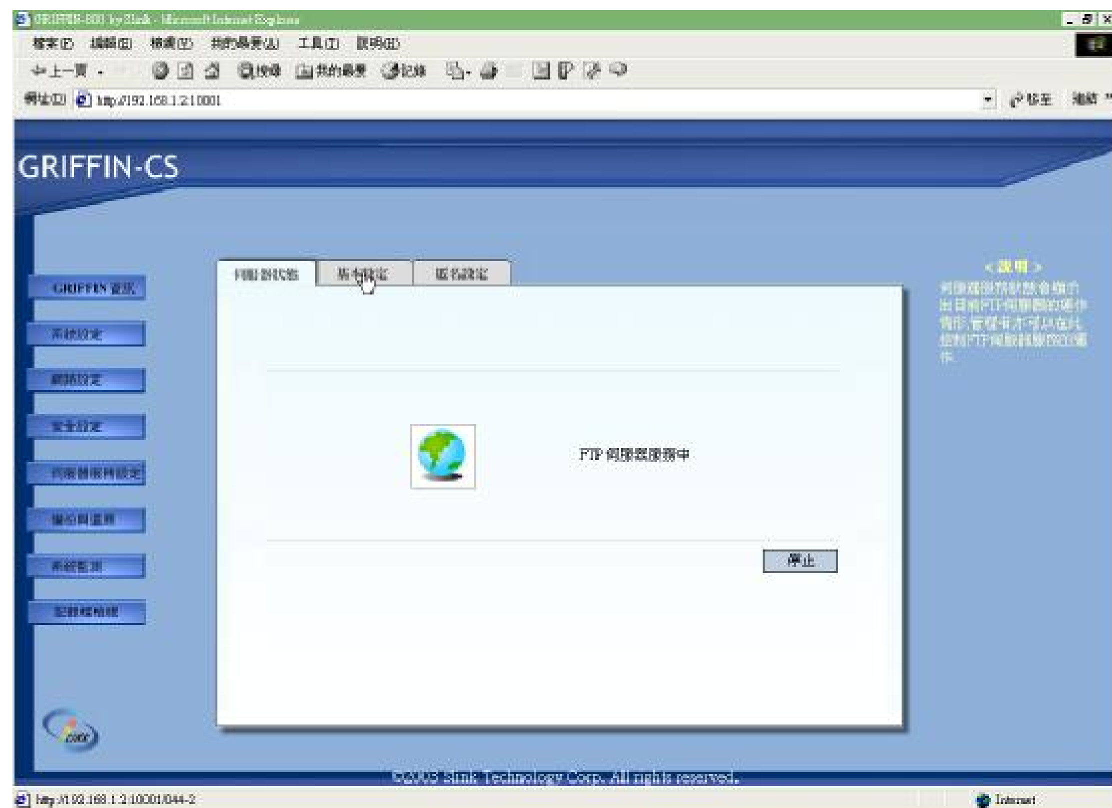


FTP 設定

FTP 設定提供企業設定檢視目前 FTP 伺服器（名稱解析伺服器）的功能，共有三小項，分述如下

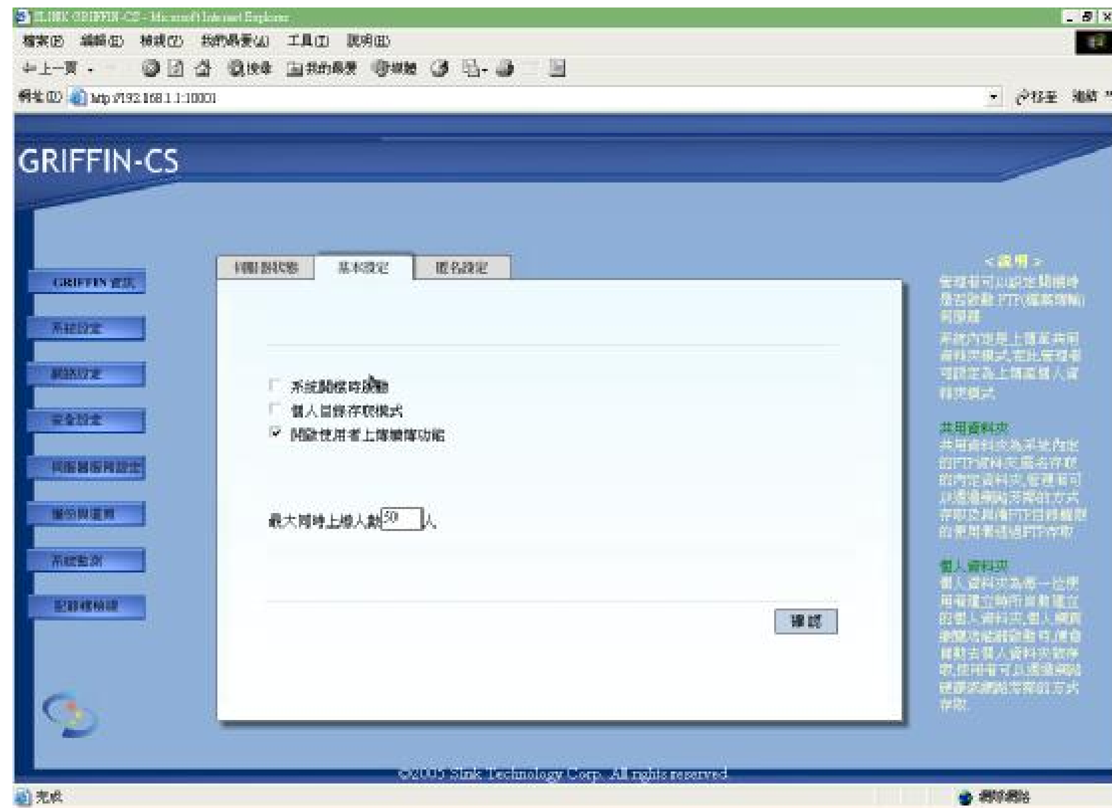
伺服器狀態

讓管理者可以監視這項網路服務的狀態，並在線上控制這項網路服務的運作，所以如果發現企業 FTP 服務有問題，則第一時間就是先檢視這網路服務有無執行。



基本設定

這裡讓管理者可以設定是否在 GRIFFIN-CS2 開機時自動啓動這項服務



GRIFFIN-CS2 所提供的 FTP 服務，有兩種模式，一爲共有檔案存取模式，另一爲個人目錄存取模式，共有檔案存取模式亦即每一位在**【使用者管理】**所設定的使用者會存取到相同的目錄（/home/ftp），其內定値爲共有檔案存取模式。

當企業有設定並啓動 SAMBA 的網路服務後，在企業的網路芳鄰中會出現本台機器，並出現 ftp_dir，這個與 FTP 服務有關的目錄出現，登錄進去後【使用者管理中對使用者需相關 windows 目錄權限】,即可直接做檔案的編輯及處理。

- 開啓開啓使用者上傳續傳功能
  GRIFFIN-CS2 可以讓 FTP 服務支援上傳續傳

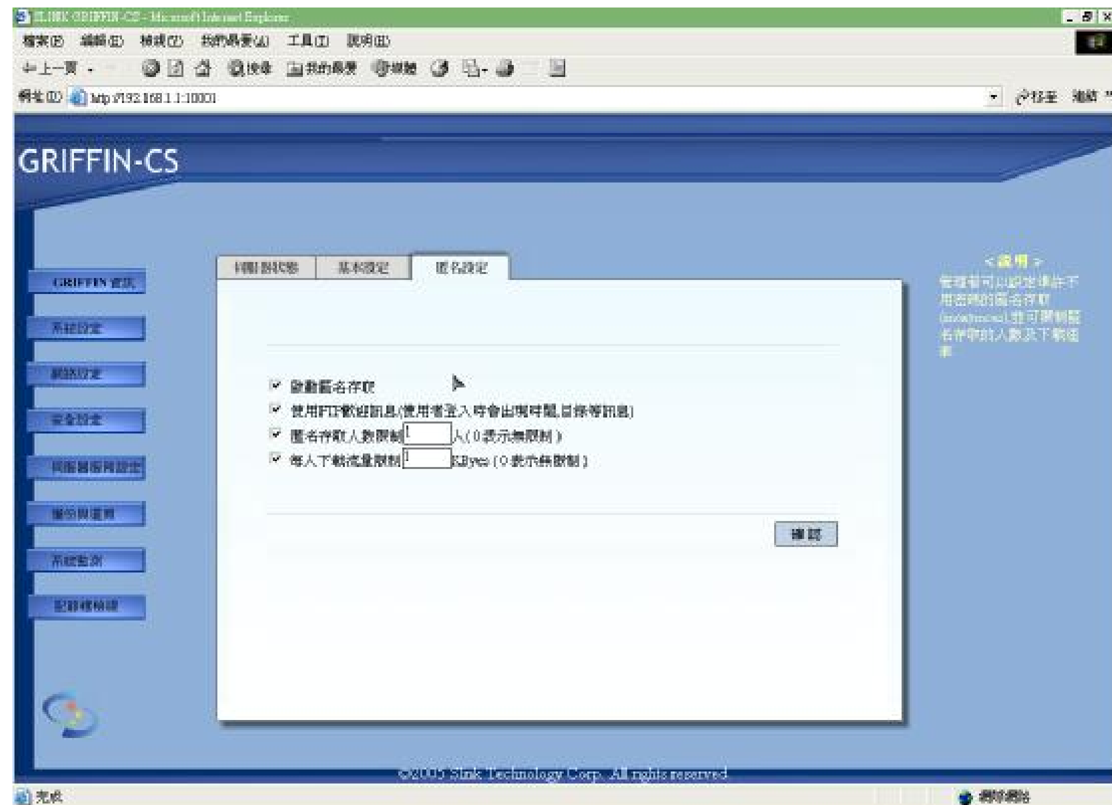
- 最大同時上線人數
  GRIFFIN-CS2 可以自訂目前最高的通時連線人數，50 爲內定値，如果您 SERVER 的效能較佳，可以將此數値訂定高一點，以增加 FTP 伺服器的最大服務人數。

n 注意

當在【**使用者管理**】中的使用者設定爲網頁目錄權限時，則其無論管理者所啓動的是任何模式，其皆會對應到/home/httpd/html/這個網頁目錄中，包含網路硬碟也會連至相同目錄，所以如果要使用的目錄存取模式爲個人，則其使用者 WINDOWS 目錄權限請勿設爲網頁目錄權限。

匿名設定

GRIFFIN-CS2 亦提供匿名存取的功能，在這邊企業可以設定是否啟動匿名存取，匿名存取最大人數，每人下載流量限制，其中匿名存取最大人數可以讓企業設定同時間使用匿名存取的最大人數，而流量限制可以讓企業設定每一位匿名存取的所可以使用的頻寬，這部分請依企業的網路頻寬做設定。



- **n** 使用 FTP 歡迎訊息

  用匿名登入 FTP 時，會出現時間,目前線上人數及目錄等訊息

SAMBA 設定

SAMBA 設定提供企業設定檢視目前 SAMBA 伺服器（名稱解析伺服器）的功能，亦可作 SAMBA 掃毒設定，共有三小項，分述如下

伺服器狀態

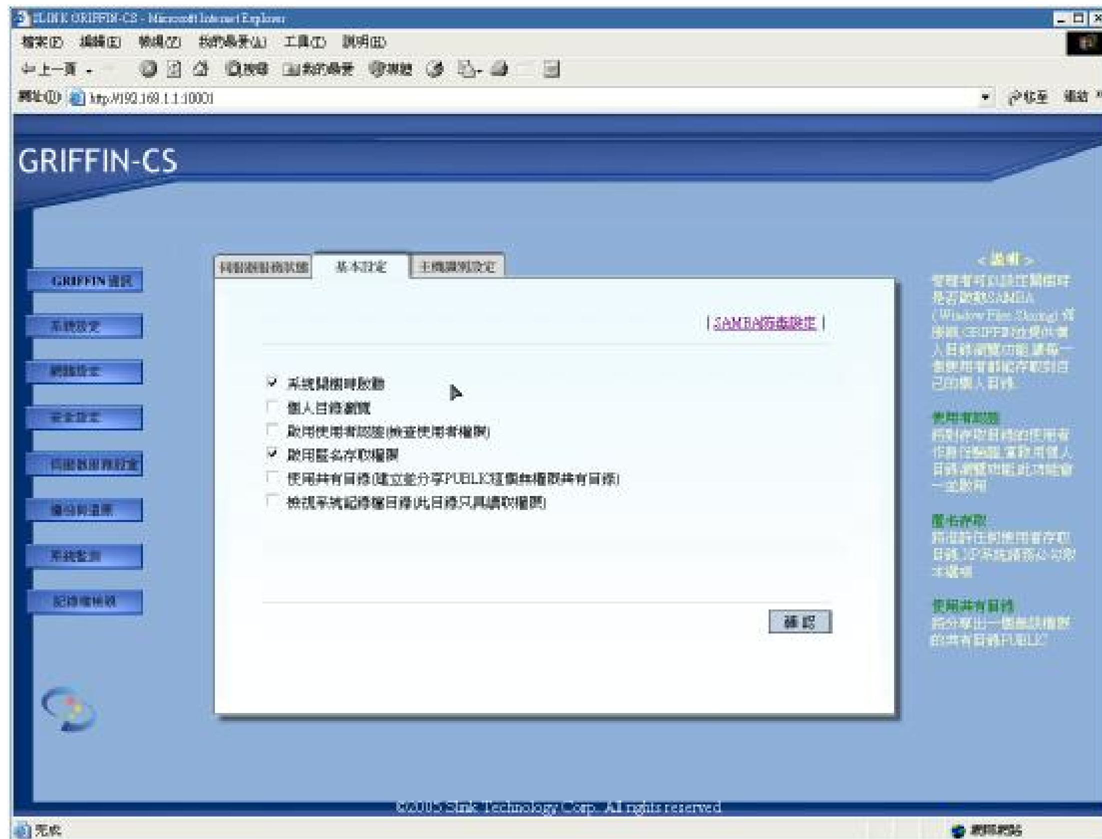
讓管理者可以監視這項網路服務的狀態，並在線上控制這項網路服務的運作，所以如果發現企業 SAMBA 服務有問題，則第一時間就是先檢視這網路服務有無執行。



如果有設定 SAMBA 防毒選項，便會依所設定的防毒服務狀況，顯示狀態。

基本設定

這裡讓管理者可以設定是否在 GRIFFIN-CS2 開機時自動啓動這項服務



- **n** 個人目錄瀏覽

  此功能需啓用使用者證功能，當使用者認證完成後，會出現自己的個人目錄，使用者可以在目錄編輯個人的網頁資料或檔案。

- **n** 使用者認證

  當使用此功能後，使用者在登錄 GRIFFIN-CS2 時，系統會要求認證，在判定使用者是否有權限存取 GRIFFIN-CS2 的分享目錄，但不使用本功能時，系統內定的目錄還是無法做存取，除非管理者亦啓用匿名存取功能。

- **n** 啓用匿名存取

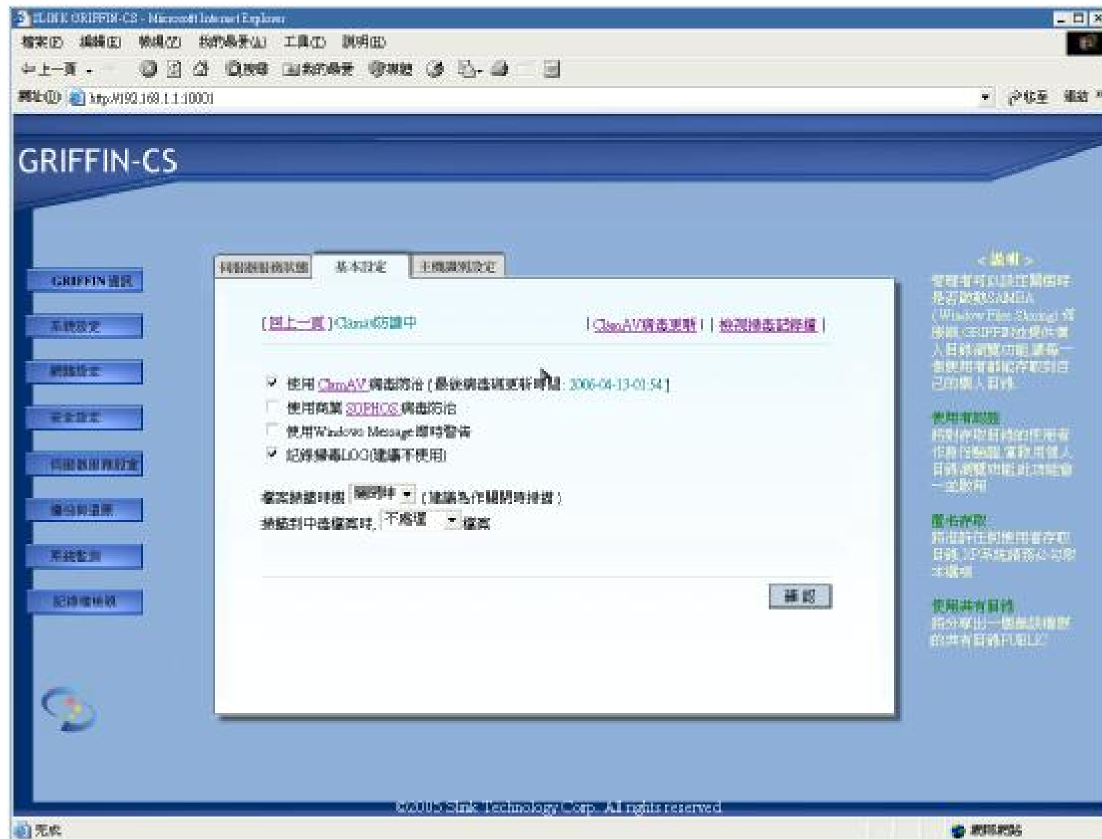
  當有啓動本功能時，任何使用者皆可以完全控制分享出來的檔案目錄，完全沒有權限控管。

- **n** 使用共有目錄

  當啓用本功能時，GRIFFIN-CS2 會建立一個沒有權限控管的目錄，任何使用者皆可以完全存取控制分享出來的檔案。

SAMBA 防毒

SAMBA 可以保護透過 SAMBA 網路芳鄰分享出去的目錄、檔案，減少被感染的機會，目前 SAMBA 防毒與郵件防毒一樣，支援 2 種防毒引擎，CLAMAV 及 SOPHOS（說明請參郵件掃描章節）。



- **n** 使用 Windows Message 即時警告

  本功能可以在掃描到檔案有病毒時，立即送一個 Windows Message 給上傳檔案的使用者。

- **n** 記錄掃毒 LOG

  記錄所有有關於 SAMBA 掃毒的記錄，使用後畫面會出現檢視病毒記錄檔功能，可以直接透過網頁檢視最近 150 筆紀錄。

- 檔案掃描時機

  可以讓您設定在何種檔案使用時機執行掃毒，是開檔、檔案關閉或是開檔、關檔皆作掃描，建議為檔案關閉時掃描，亦即有檔案寫入時在做掃描。

- 中毒檔案處理方式

  可以讓您設定掃描到病毒時，要如何處理有病毒感染的檔案

  不處理

  不作任何處理

  刪除

  直接刪除

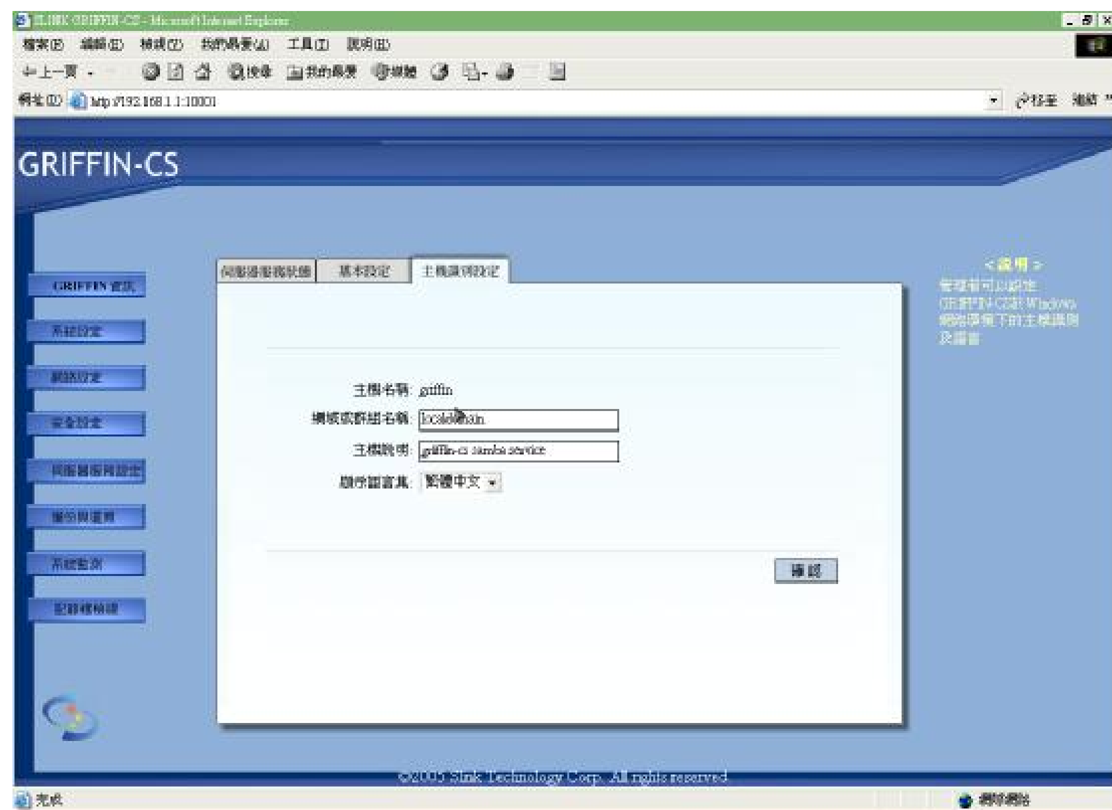
  隔離

  隔離到/var/tmp/virus 這個目錄，選擇本處理方式時，SAMBA 也會將/var/tmp/virus 這個目錄分享出來。

主機識別設定

這裡提供管理者設定 GRIFFIN-CS2 在 Windows 網路芳鄰中要顯示的資訊，設定資料說明如下表

項目	說明
主機名稱	在網路芳鄰 GRIFFIN-CS2 所出現的名稱
網域或群組名稱	企業網路所屬網域，群組，內定爲 WORKGROUP
主機說明	在網路芳鄰 GRIFFIN-CS2 所出現的說明
顯示語言	可以視您所在使用者端的區域，選擇顯示的語言，內定爲繁體中文

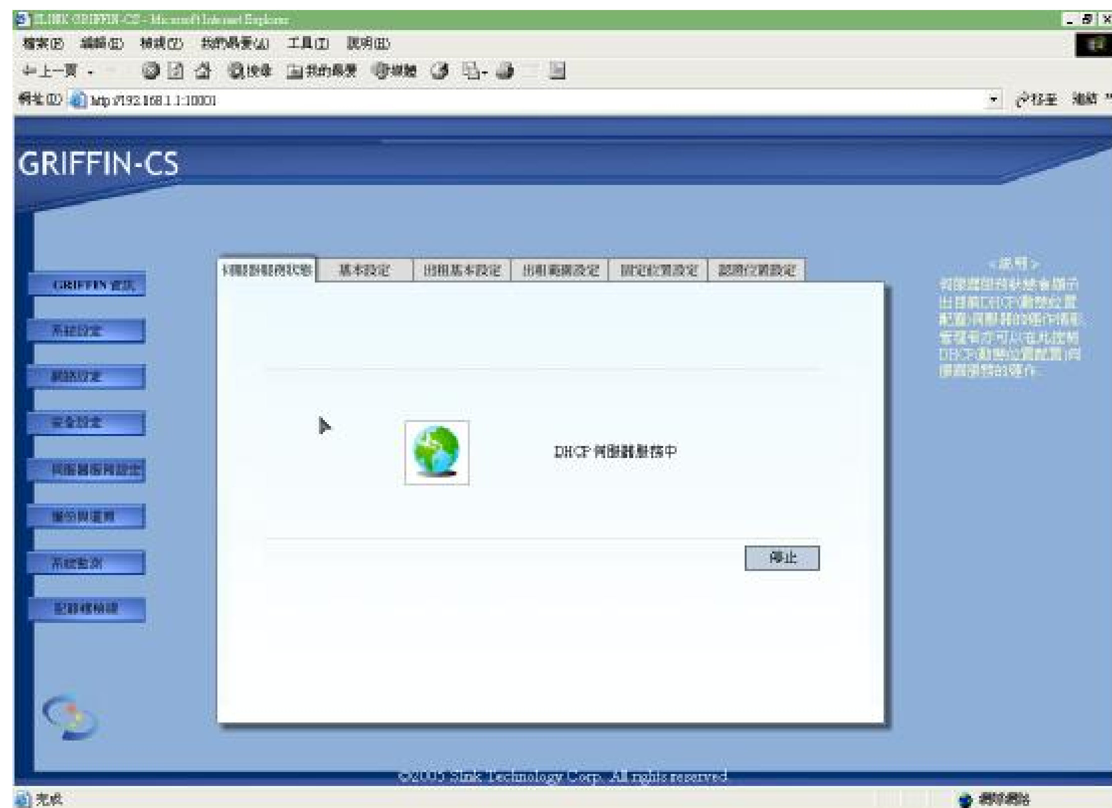


DHCP 設定

DHCP 設定提供企業設定檢視目前 DHCP 伺服器（名稱解析伺服器）的功能，共有六小項，分述如下

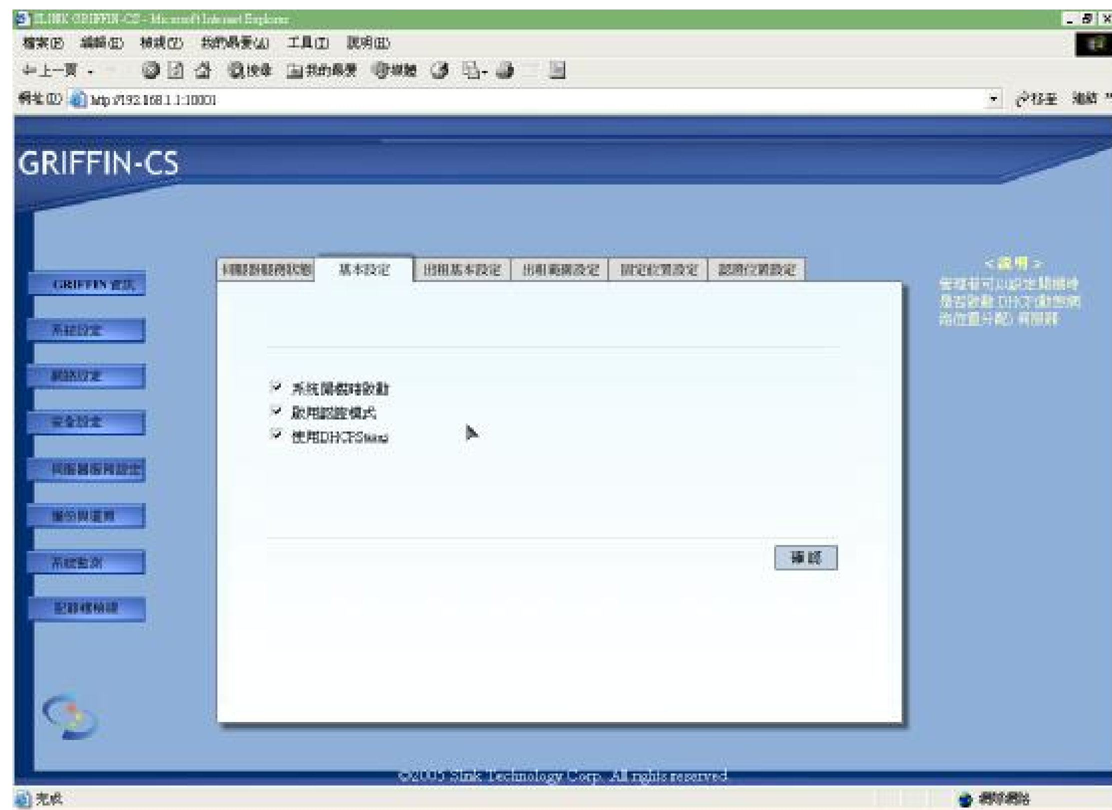
伺服器狀態

讓管理者可以監視這項網路服務的狀態，並在線上控制這項網路服務的運作，所以如果發現企業 DHCP 服務有問題，則第一時間就是先檢視這網路服務有無執行。



基本設定

這裡讓管理者可以設定是否在 GRIFFIN-CS2 開機時自動啟動這項服務



- **n** 啟用認證模式

  這個選項可以讓您管控在 DHCP 服務，使用者自動取得情形，主要便是對個使用者電腦的網路卡 MAC 位置做管控，不在允許的使用者電腦，將無法自動取的網路位置，詳細設定請參考認證位置設定章節。

- 使用 DHCPStatus

GRIFFIN-CS2 內建 DHCPStatus 程式，可以幫助您了解目前 DHCP 伺服器的租約狀態，幫助管理。

DHCP Subnet Information

Location	Subnet	Netmask	IP range	Router	IPs defined	IPs used	IPs free
	[illegible]	[illegible]	[illegible]	[illegible]	0	0	0
	192.168.1.0	255.255.255.0	[illegible] - 192.168.1.254	192.168.[illegible]	[illegible]	0	[illegible]

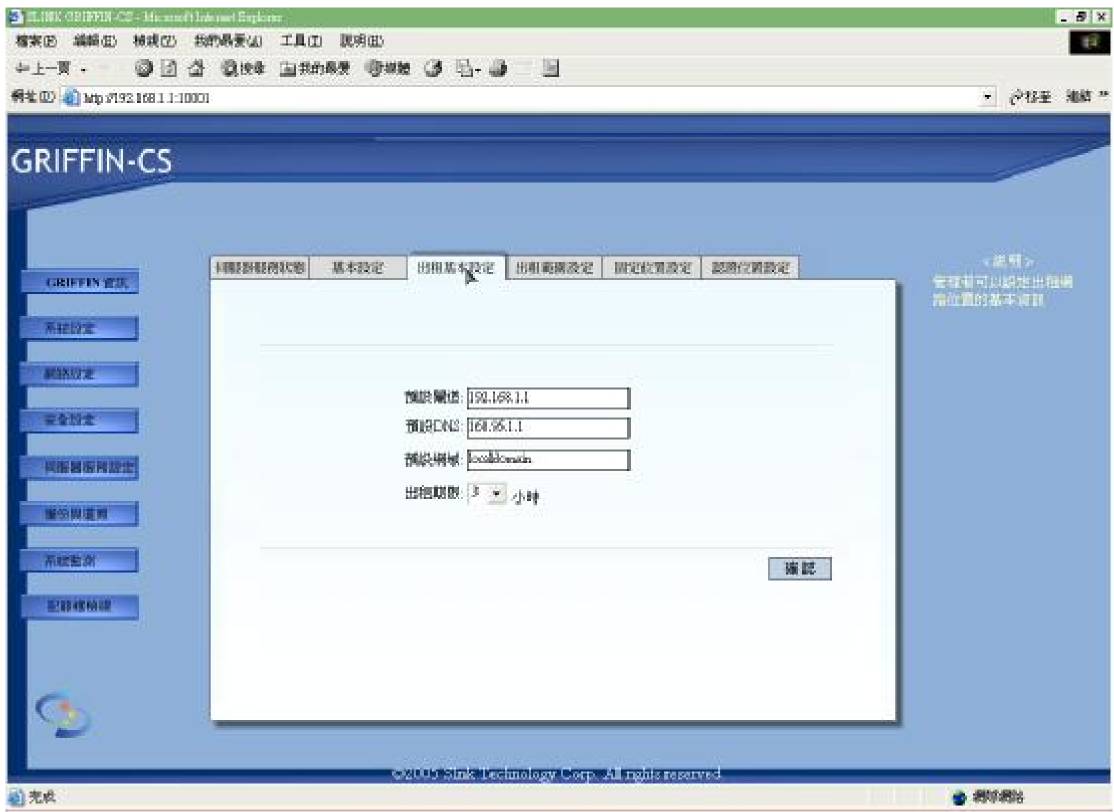
DHCP Subnet Information

Subnet:	192.168.1.0	Netmask:	255.255.255.0
Broadcast:		Router:	192.168.1.1
DNS servers:	[illegible]	WINS servers:	
IP range:	192.168.1.[illegible] - 192.168.1.[illegible]	--	--

IP address	Lease status	Lease start	Lease end	Mac address	DNS name	WINS name
192.168.1.100	Free					
192.168.1.101	Free					
192.168.1.102	Free					
192.168.1.103	Free					
192.168.1.104	Free					
192.168.1.105	Free					
192.168.1.106	Free					
192.168.1.107	Free					
192.168.1.108	Free					
192.168.1.109	Free					
192.168.1.110	Free					
192.168.1.111	Free					
192.168.1.112	Free					

位置出租設定

這裡讓管理者設定 DHCP 基本所要的網路位置資訊



各欄位說明如下

項目	說明
預設閘道	出租網路設定的網路閘道位置
預設 DNS	出租網路設定的網路 DNS 位置
預設網域	出租網路設定的網路網域
出租期限	網路位置的出租期限，以小時計算

出租範圍設定

GRIFFIN-CS2 可讓企業設定多個 DHCP 的範圍對應，包含不同的網路區段及 DNS、閘道、及 WINS 等



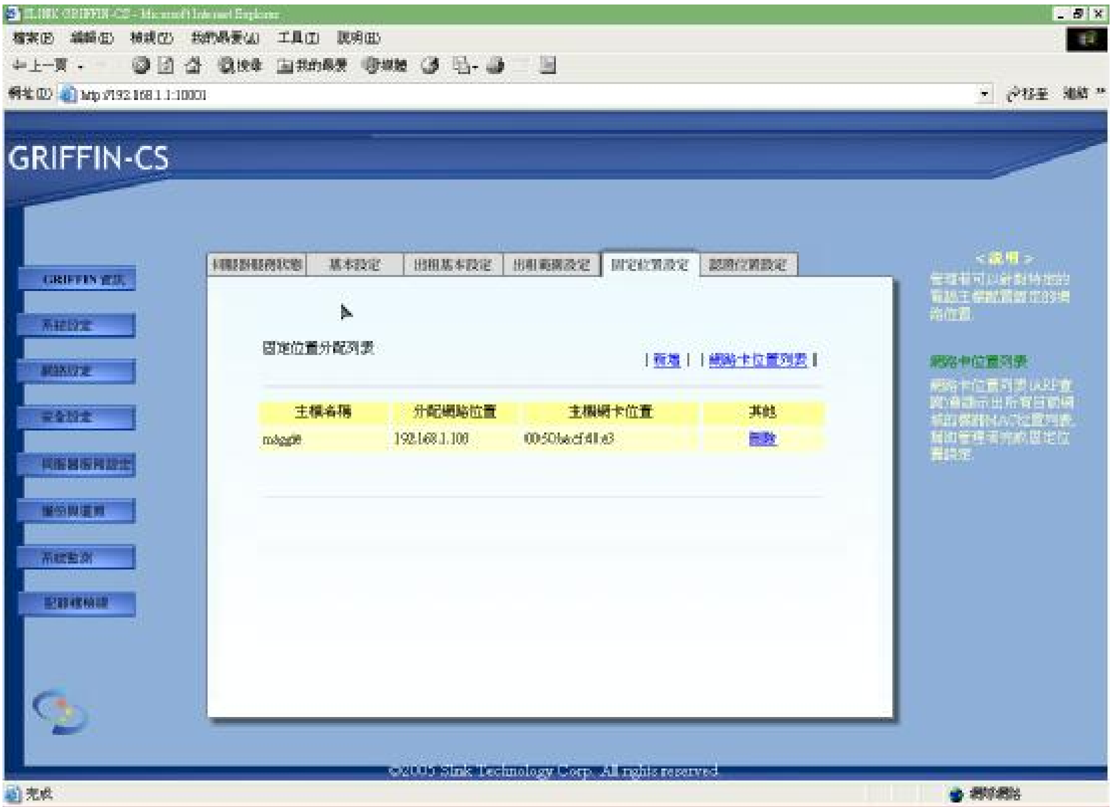
注意

當網路設定精靈執行成功後，會自動幫 GRIFFIN-CS2 產生一筆對外的空的範圍資料，請勿刪除本筆資料，否則將無法正常啓動 DHCP。

當 DNS 位置、閘道、網域名稱未輸入時，則會採用【出租基本設定】中的基本設定值。

固定位置設定

GRIFFIN-CS2 可讓管理者爲特別的電腦分配固定的網路位置，其中亦提供一個簡易的網路卡位置查詢功能，會列出網路上電腦的網路卡 MAC 位置，以方便管理者設定



認證位置設定

當您在基本設定中，啟用 DHCP 認證設定時，所有使用者電腦的 MAC 位置，如果不在 DHCP 使用者列表中，便無法透過 DHCP 自動取得網路位置。



備份與還原

備份與還原為 GRIFFIN-CS2 所提供的備份精靈與還原精靈的功能，可以讓管理者備份 GRIFFIN-CS2 的資料，並將備份過的資料還原，以確保資料異常時能夠將 GRIFFIN-CS2 還原。

GRIFFIN-CS2 提供網路芳鄰及 FTP 遠端主機的備份。

備份精靈

備份精靈提供兩種備份的方式，立即備份與排程備份，功能兩者皆一樣，只是立即備份是線上立即執行，完成，排程備份則是由管理者自行訂定備份的時間，所有備份完成皆會寄一封確認信給管理者，並留下記錄。



如果要備份到網路芳鄰或 FTP 遠端主機，請先完成遠端資料設定。

備份種類

GRIFFIN-CS2 目前提供的備份形式爲完全備份及增量備份，目前有四種備份種類，分別說明如下

<table>
<tr><td>全部</td><td colspan="2">會備份執行系統備份、資料庫備份、及 Web 網頁備份</td></tr>
<tr><td rowspan="12">系統</td><th>名稱</th><th>詳細說明</th></tr>
<tr><td>GRIFFIN 設定檔</td><td>griffin 的設定檔</td></tr>
<tr><td>系統使用者設定檔</td><td>使用者設定檔，群組設定檔</td></tr>
<tr><td>FTP 設定檔</td><td>FTP 伺服器的設定檔</td></tr>
<tr><td>MAIL 設定檔</td><td>MAIL 伺服器的設定檔，使用者郵件資料</td></tr>
<tr><td>郵件掃描設定檔</td><td>郵件掃描設定檔</td></tr>
<tr><td>垃圾郵件防治設定檔</td><td>垃圾郵件防治設定檔</td></tr>
<tr><td>入侵偵測設定檔</td><td>入侵偵測設定檔</td></tr>
<tr><td>WEB 設定檔</td><td>WEB 伺服器的設定檔</td></tr>
<tr><td>SAMBA 設定檔</td><td>SAMBA 伺服器的設定檔</td></tr>
<tr><td>IDS 設定檔</td><td>IDS 保護設定檔</td></tr>
<tr><td>DHCP 設定檔</td><td>DHCP 伺服器的設定檔</td></tr>
<tr><td>HOME 目錄</td><td colspan="2">備份整個 HOEM（各使用者資料）下面資料，含 CGI 程式</td></tr>
<tr><td>MYSQL 網頁</td><td colspan="2">備份整個 WEB 網頁內容，含 CGI 程式</td></tr>
<tr><td>POSTGRESQL 網頁</td><td colspan="2">備份整個 WEB 網頁內容，含 CGI 程式</td></tr>
<tr><td>Web 網頁</td><td colspan="2">備份整個 WEB 網頁內容，含 CGI 程式</td></tr>
</table>

命名方式

GRIFFIN-CS2 的備份檔案命名規則有兩種，一種爲自行輸入，另一種爲自動產生依據目前備份時間產生，如 2003 年 1 月 1 日 13 時，則會產生 2003010113.tgz 的檔名，而檔案的最前面則爲備份種類

名稱	說明
all	代表全部備份檔案
sys	代表系統備份檔案
home	代表 HOME 資料備份檔案
mysql	代表 MYSQL 備份檔案
pgsql	代表 POSTGRESQL 備份檔案
web	代表網頁備份檔案

所以如果企業於 2003 年 1 月 1 日 13 時執行全部備份，則自動會產生備份檔案爲 all-2003010113.tgz。

備份的檔案會存於/home/backup 中，如管理者有啓動 SAMBA，則會對應到網路芳鄰上 GRIFFIN-CS2 的 backup，當然管理者必須有權限才可以存取這個目錄。

注意

如果管理者選擇檔名系統產生，則兩次備份時間間隔，請勿小於一小時。

增量備份

當 GRIFFIN-CS2 執行過第一次的完整備份後，其系統會做一個時間記錄，當下次要在執行備份時，便會出現增量備份這個選項，並會自動計算上次備份到今天的時間天數，完成增量備份。

當 GRIFFIN-CS2 執行完第一次增量備份後，下次的增量備份選項便會出現距上次完整備份及上次增量備份的選項供管理者選擇。

注意

GRIFFIN-CS2 會對每種一備份種類做不同的時間記錄，不同種類的備份，其對 GRIFFIN-CS2 來說皆爲不同的備份記錄，還句話說，當執行完成全部的完整備份，當你下次備份選擇完整備份時，會出現增量備份選項，但如果備份種類選擇爲 WEB 網頁時,則不會出現增量備份選項,因對 GRIFFIN-CS2 而言,它是一次完全部不同的備份記錄。

還原精靈

還原精靈提供管理者一個相當容易的方式去做資料還原，你只要依照精靈指示即可相當容易的還原 GRIFFIN-CS2 的資料。



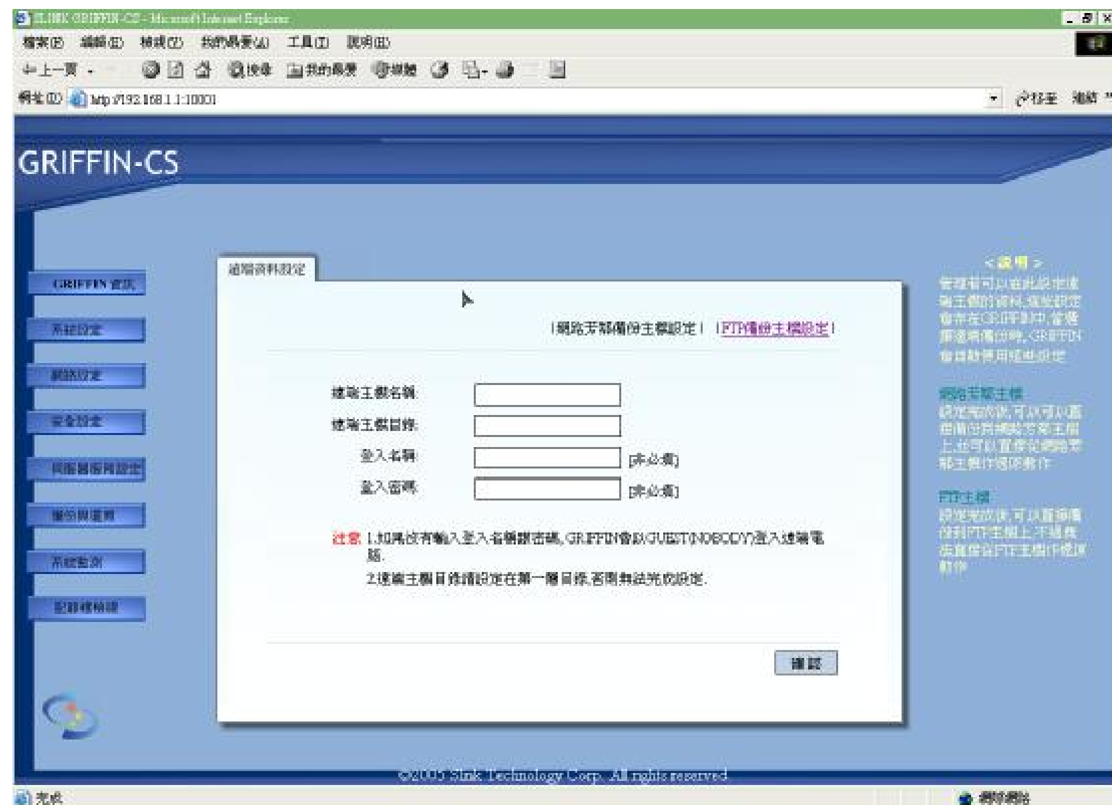
還原精靈會依管理者選擇的備份種類去/home/backup 目錄找尋，符合的備份檔名，並依管理者所選擇的檔名完成資料還原。

如果選擇的還原種類爲全部或系統時，記得還原完畢後，要重新開機喔!

遠端資料設定

GRIFFIN-CS2 遠端資料設定可以設定網路芳鄰主機及 FTP 遠端主機，分別說明如下

網路芳鄰主機



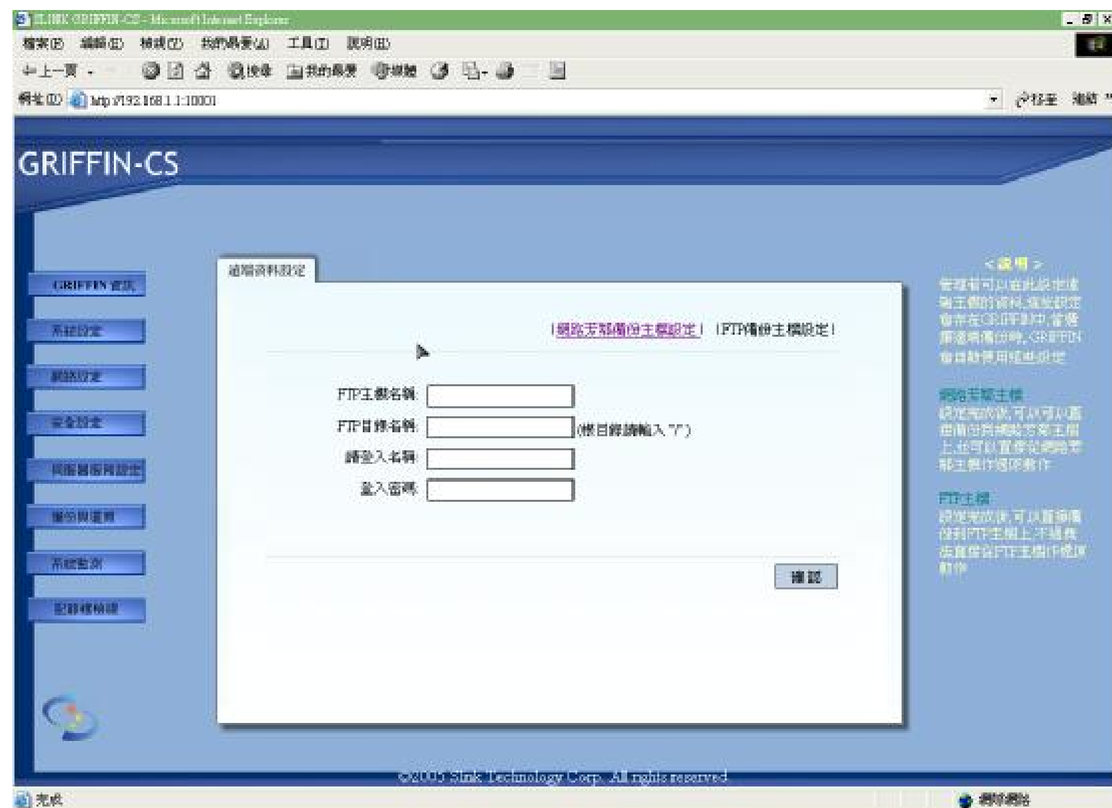
這裡需輸入遠端的主機名稱，他提供的是以網路芳鄰的方式經資料送出，所以輸入的主機名稱需先在網路芳鄰中可以找到，才可以完成設定，

假設企業有一台 NAS 主機叫 backup_center，然後你建立了一個 backup 的目錄，所以在網路芳鄰莊會見到 backup_center 這台這主機，會有一個目錄叫 backup，那在遠端資料設定中，遠端的主機名稱輸入 backup_center（勿輸入\\backup_center），遠端的主機目錄輸入 backup（勿輸入\backup）即可。

按下確定後，請等待幾秒，系統會自動取找尋這台機器，如果可以找尋到，才會完成設定。

如果登入名稱及登入密碼沒有輸入，則 GRIFFIN-CS2 會以 guset/guest 做登入的名稱及密碼。

FTP 遠端主機



這裡需輸入遠端 FTP 的主機名稱或網路位置，FTP 目錄名稱請輸入要備份的目錄即可，如果在根目錄下則輸入"/"。

按下確定後，請等待幾秒，系統會自動使用設定的資訊，登入到遠端 FTP 中，如果可以找尋並登入成功，才會完成設定。

系統監測

GRIFFIN-CS2 提供管理者設定系統警示的條件及要監測網路服務，並可線上監視 GRIFFIN-CS2 的的 CPU 使用率、記憶體使用率、及網路流量報表。

系統警示設定

GRIFFIN-CS2 提供管理者監控目前中央處理器、記憶體、網路流量及硬碟容量的使用率狀態，並可針對各項監控設定警示發送的標準

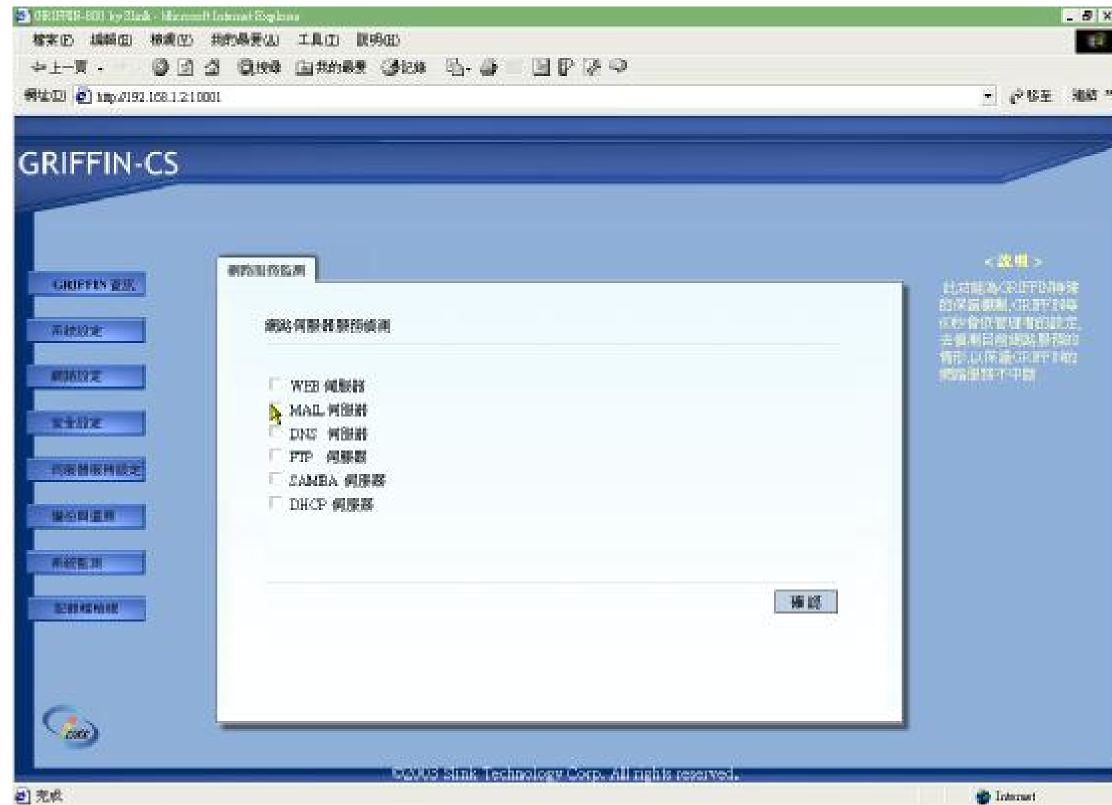


GRIFFIN-CS2 的後端偵測技術會根據上述設定，每 60 秒偵測系統一次，當超出管理者所設定的標準時，依情況發出警示訊息。

當管理者使用虛擬網路的功能時，這邊也可以讓管理者清楚目前網路卡的運作狀態，

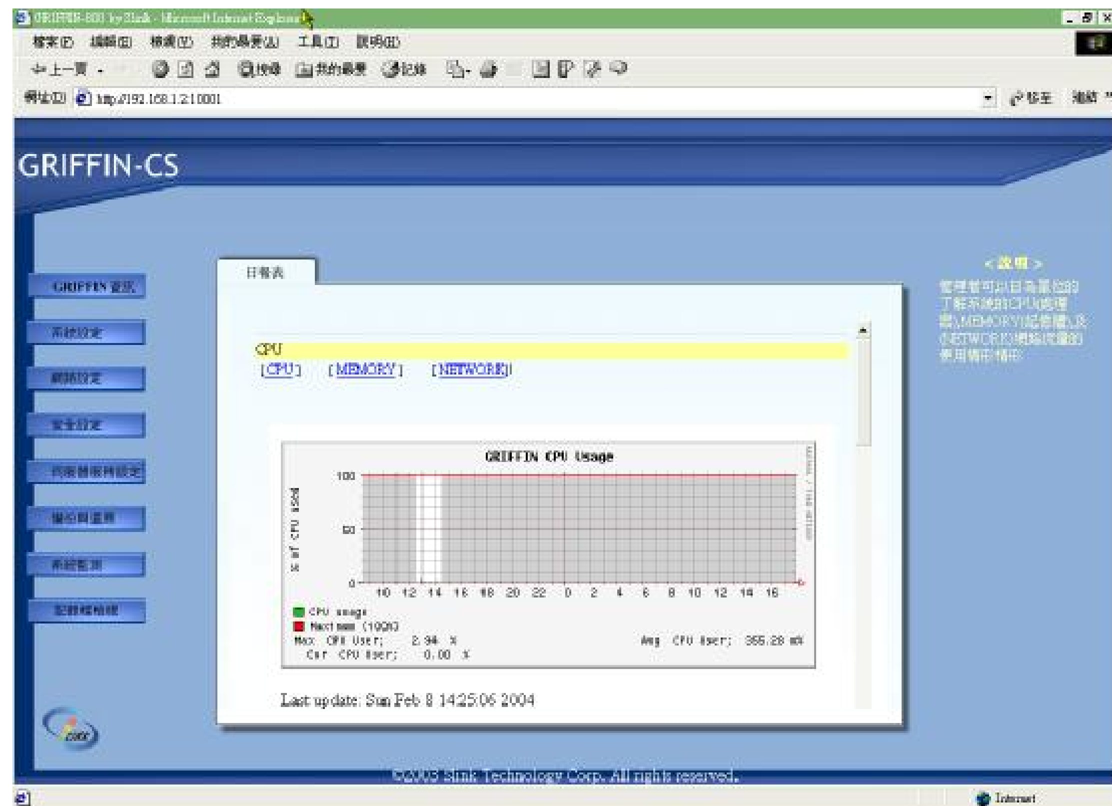
網路服務監測

GRIFFIN-CS2 亦提供一個對網路服務的保護機制，管理者可以針對目前企業的需求，針對重要的網路服務進行保護，當監控的網路服務莫名被停止，本機制會自動的將監控的網路服務重新啓動，以確保此網路服務的不斷運作。



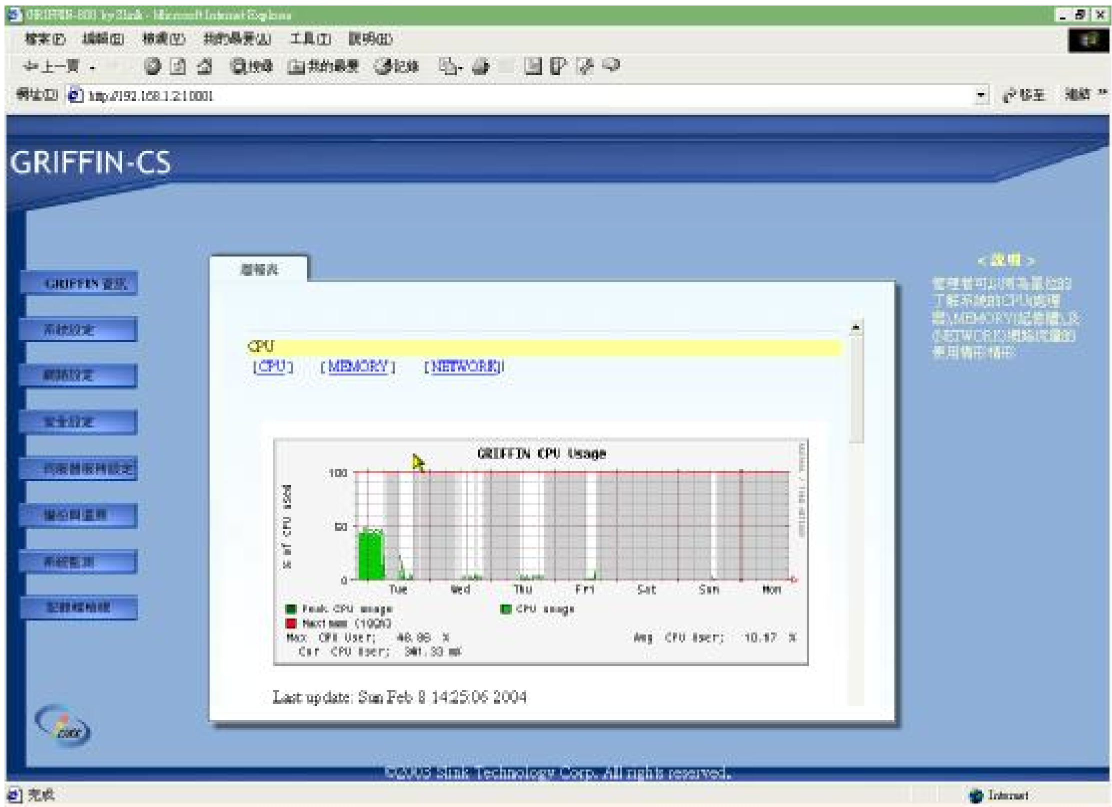
日報表

以日為基礎的監測 GRIFFIN-CS2 的系統，讓管理者可以相當容易的了解到今天 CPU 的使用率、記憶體的使用率、及網路的流量資訊等。



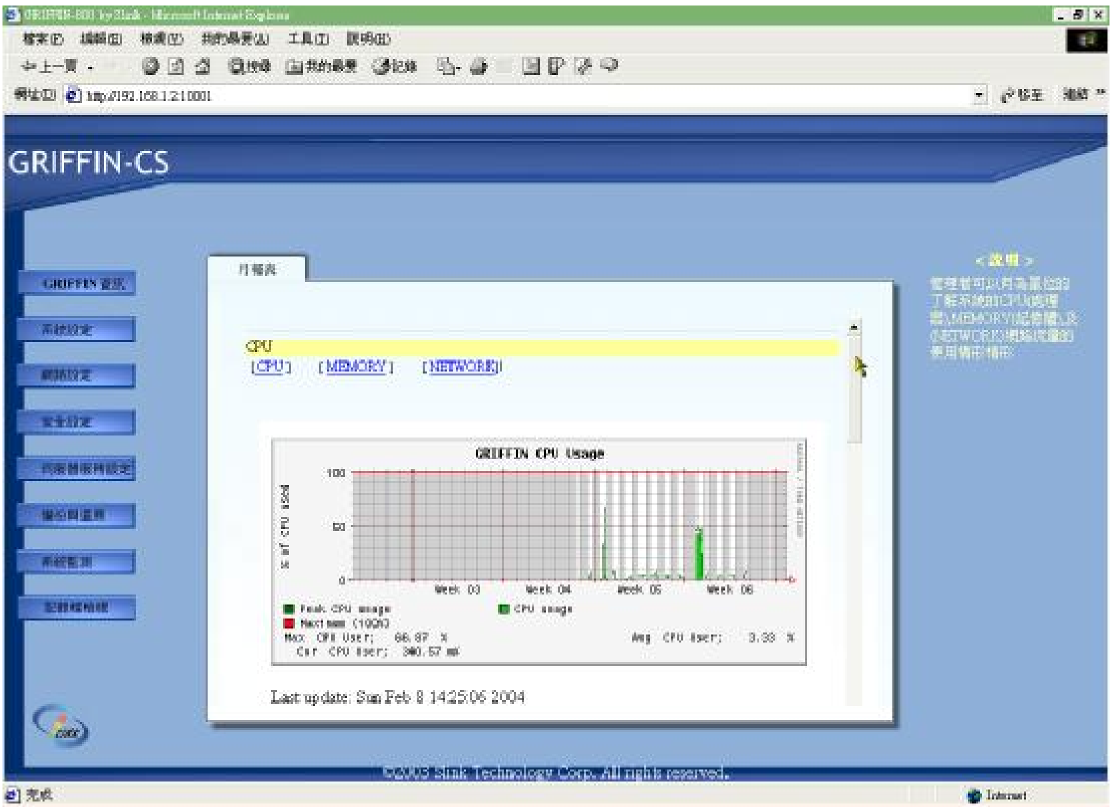
週報表

以週為基礎的監測 GRIFFIN-CS2 的系統，讓管理者可以相當容易的了解到今天 CPU 的使用率、記憶體的使用率、及網路的流量資訊等。



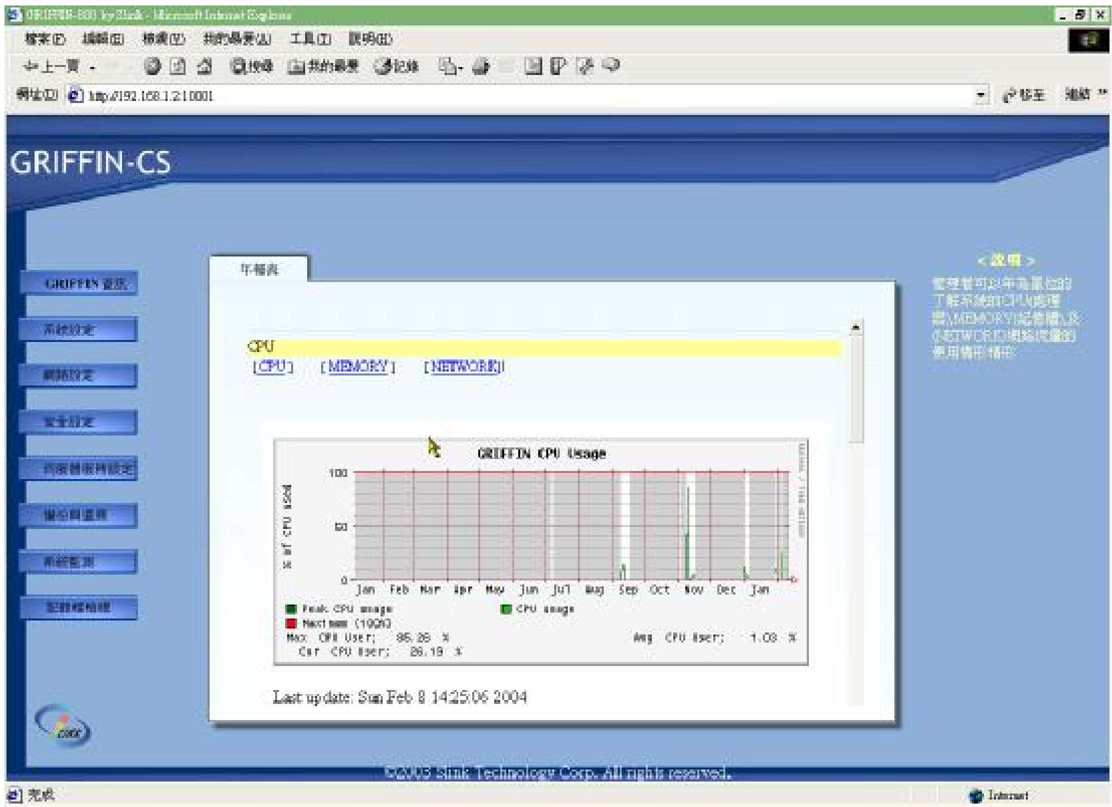
月報表

以月為基礎的監測 GRIFFIN-CS2 的系統，讓管理者可以相當容易的了解到今天 CPU 的使用率、記憶體的使用率、及網路的流量資訊等。



年報表

以年爲基礎的監測 GRIFFIN-CS2 的系統，讓管理者可以相當容易的了解到今天 CPU 的使用率、記憶體的使用率、及網路的流量資訊等。



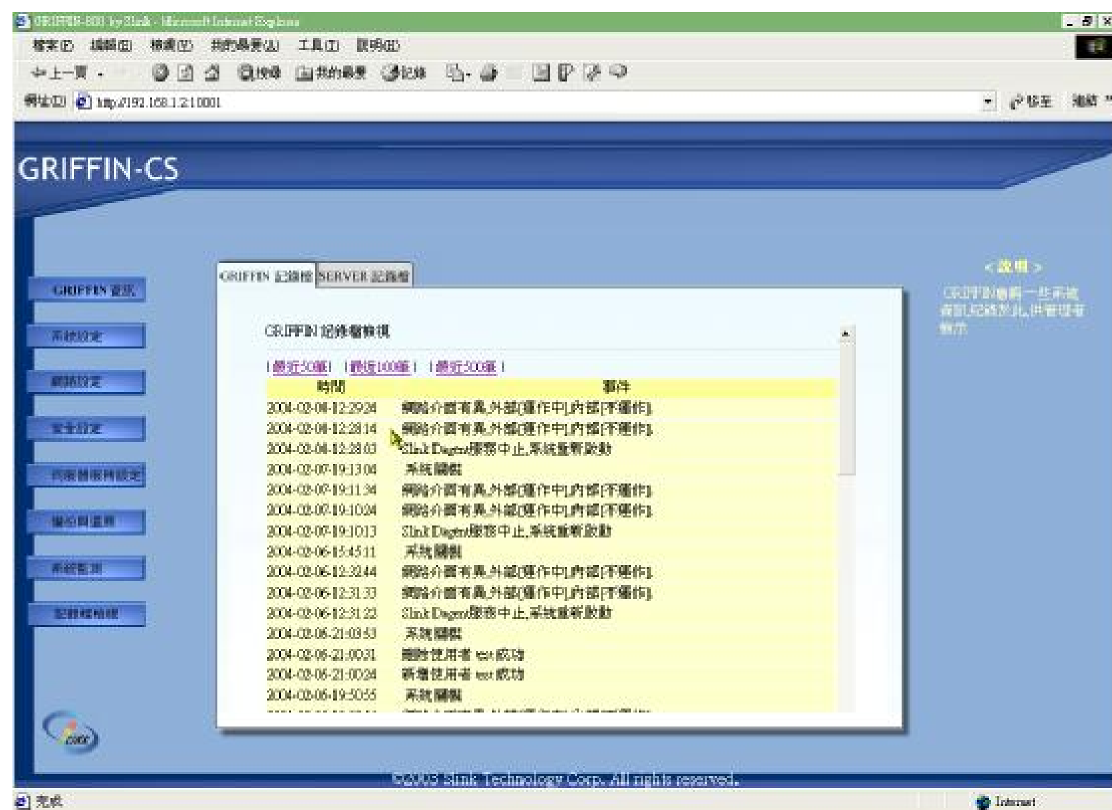
記錄檔檢視

GRIFFIN-CS2 的記錄檔檢視功能提供兩大系統記錄功能，包含主機記錄檔及郵件記錄檔，以幫助管理者管理了解目前 GRIFFIN-CS2 的資訊

系統記錄檔

GRIFFIN 記錄檔

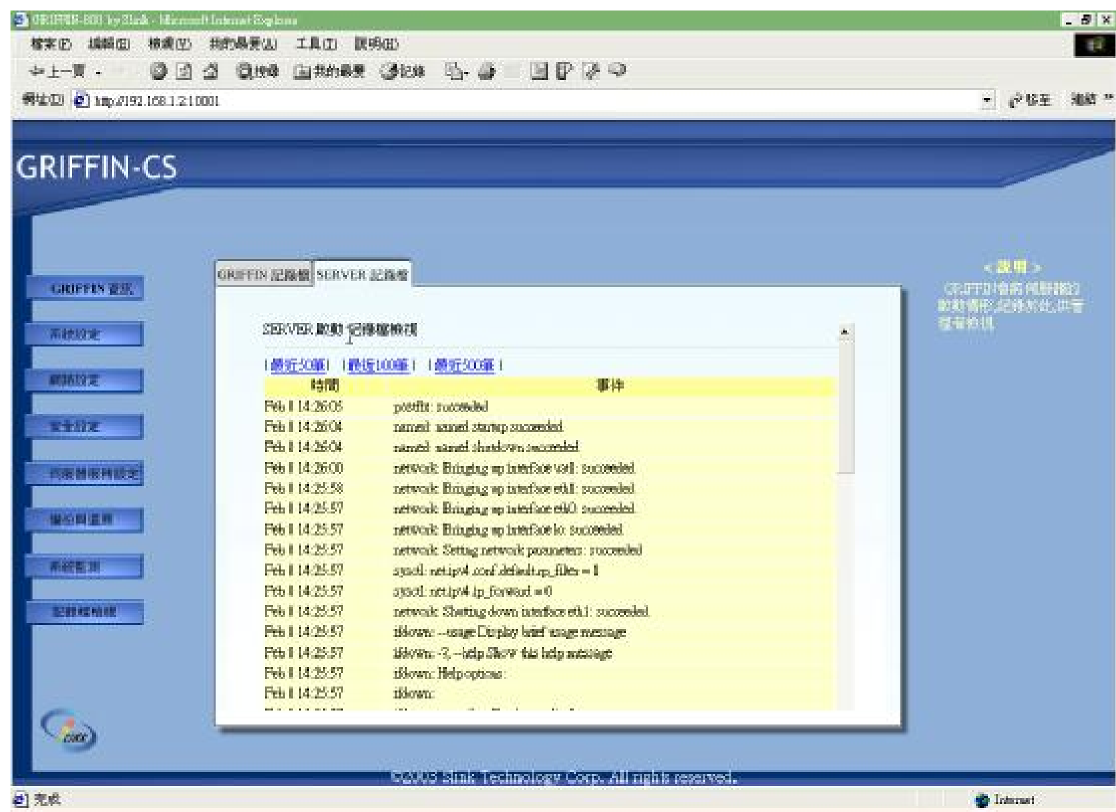
GRIFFIN 紀錄檔提供管理者清楚的 GRIFFIN-CS2 相關事件的紀錄，如使用者新增記錄、密碼變更記錄、系統更新記錄、系統備份記錄等。



管理者可依需求檢視最近 50 筆、100 筆或 500 筆記錄。

SERVER 記錄檔

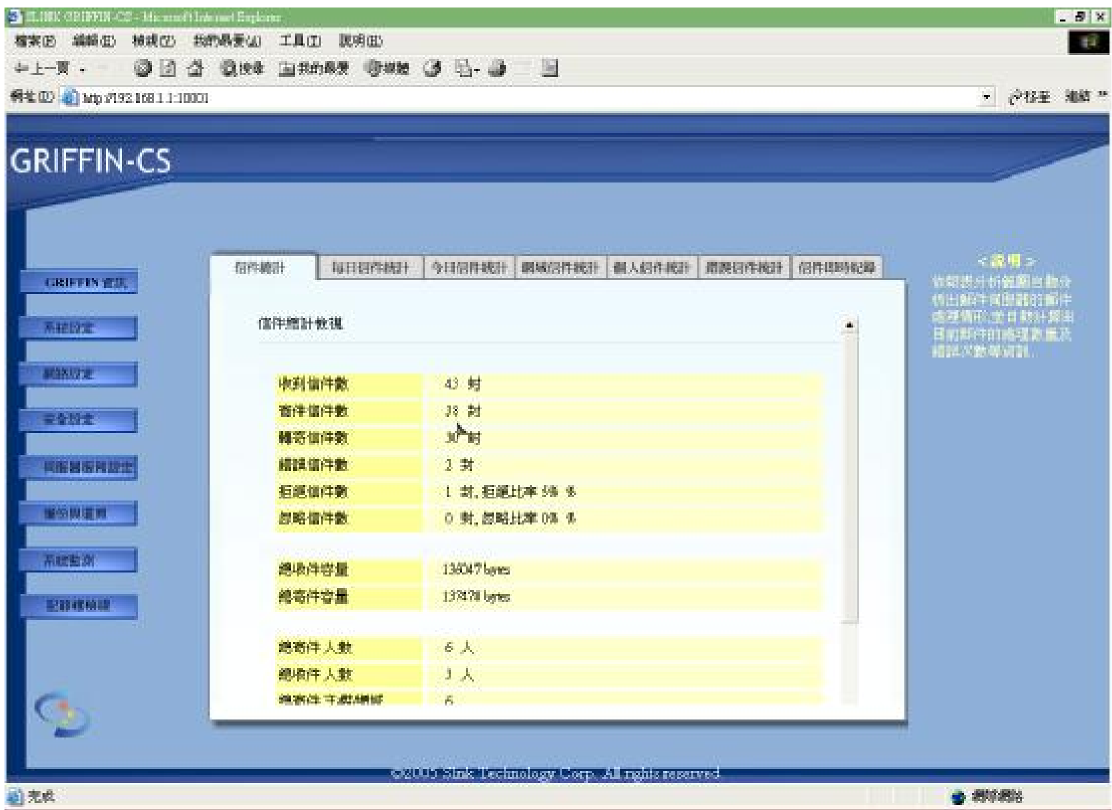
SERVER 記錄檔供管理者檢視 GRIFFIN-CS2 所有網路服務的開機啓動狀態。



郵件記錄檔

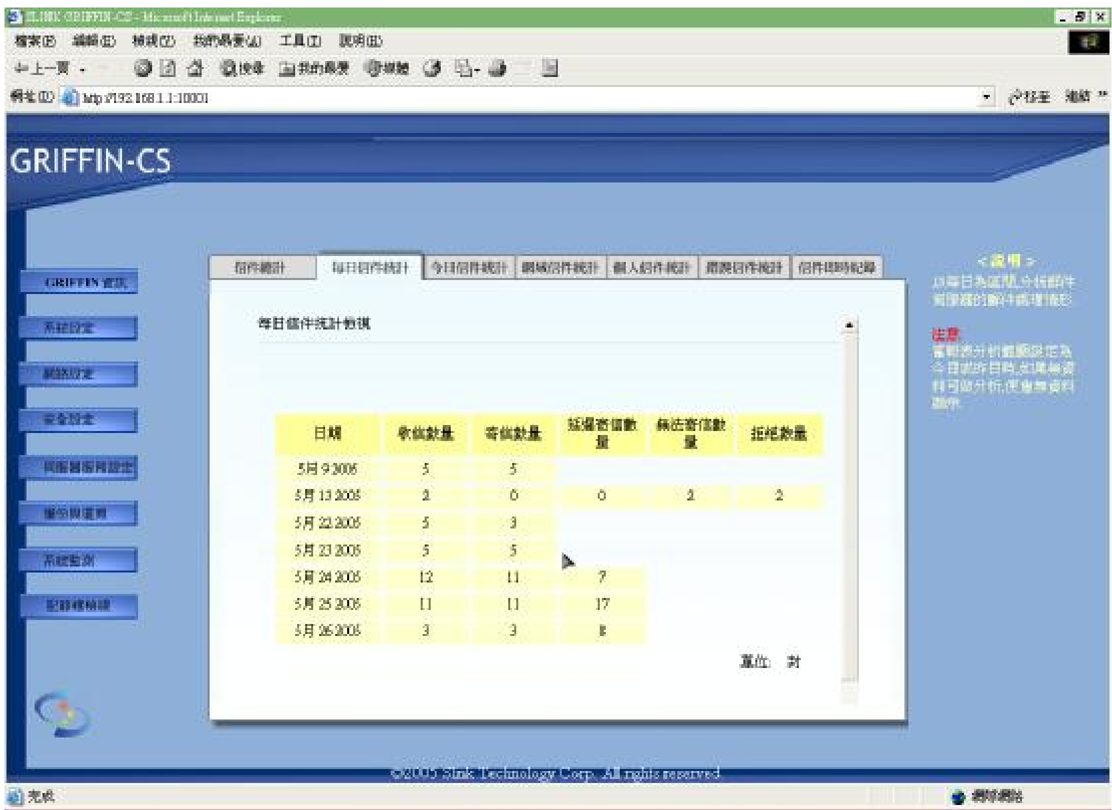
信件總計

信件總計會依郵件基本設定中所設定的報表分析範圍做出郵件的總分析，如在此時間區段中有多少信件寄送，有多少問題發生等，做一總表統計。



每日信件統計

以日為時間單位，統計出每日的郵件寄送量



注意

當報表分析範圍設定為今日或昨日時，無資料時便會顯示無資料可顯示

今日信件統計

以每小時為時間單位，統計出每小時的郵件寄送量

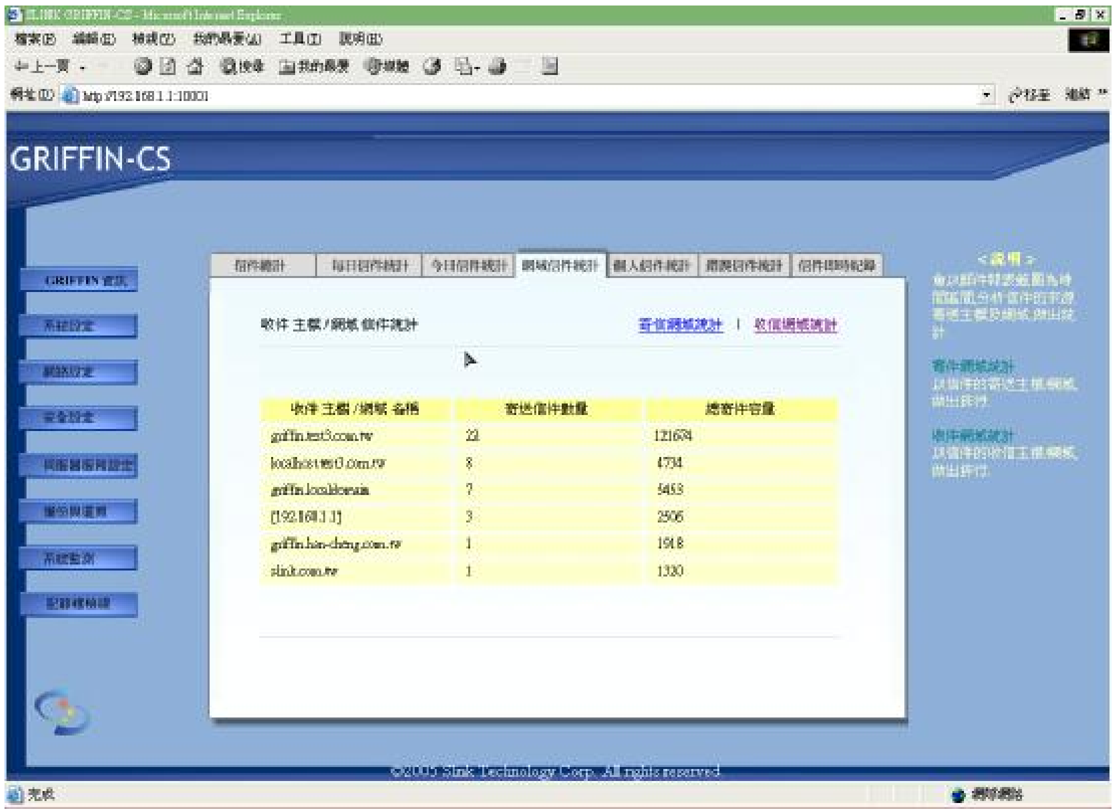


網域信件統計-寄信網域統計

以寄信目的的網域為單位，統計出那個網域的郵件寄件的數量、平均寄送的時間等，可以相當簡易的了解 GRIFFIFN-CS 寄送到哪個網域的信件最多

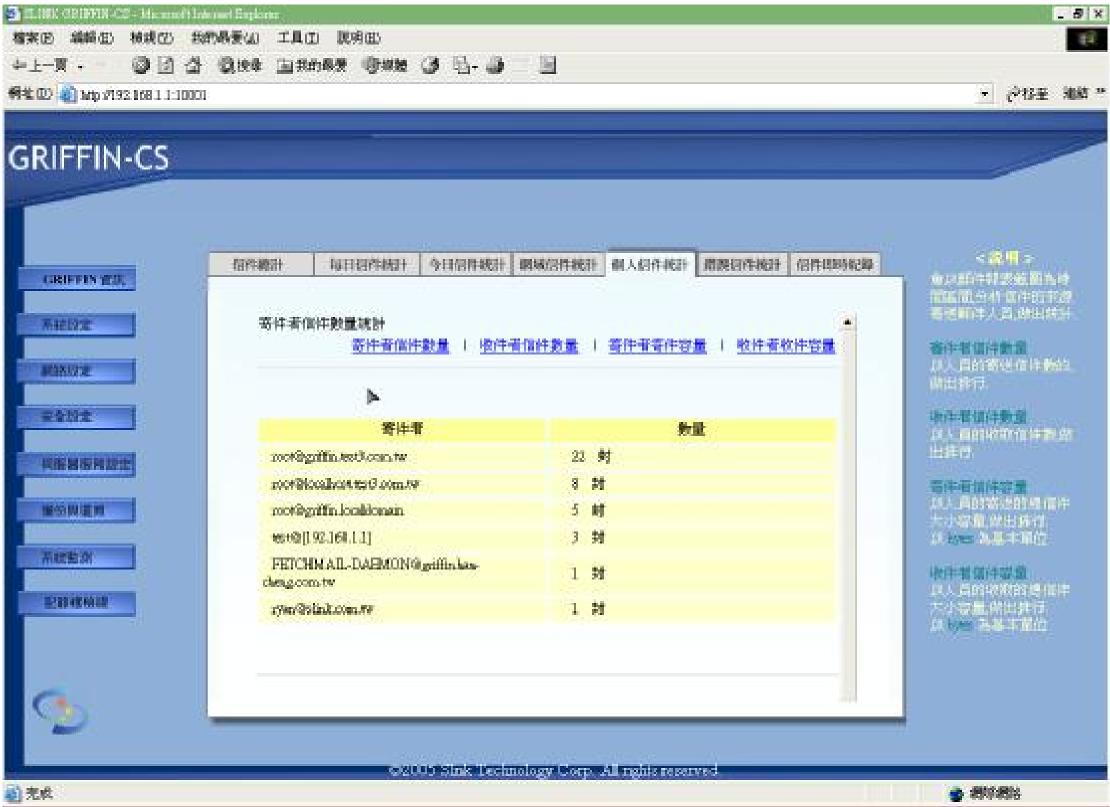
網域信件統計-收信網域統計

以網域為單位，統計出哪個網域的收件最多



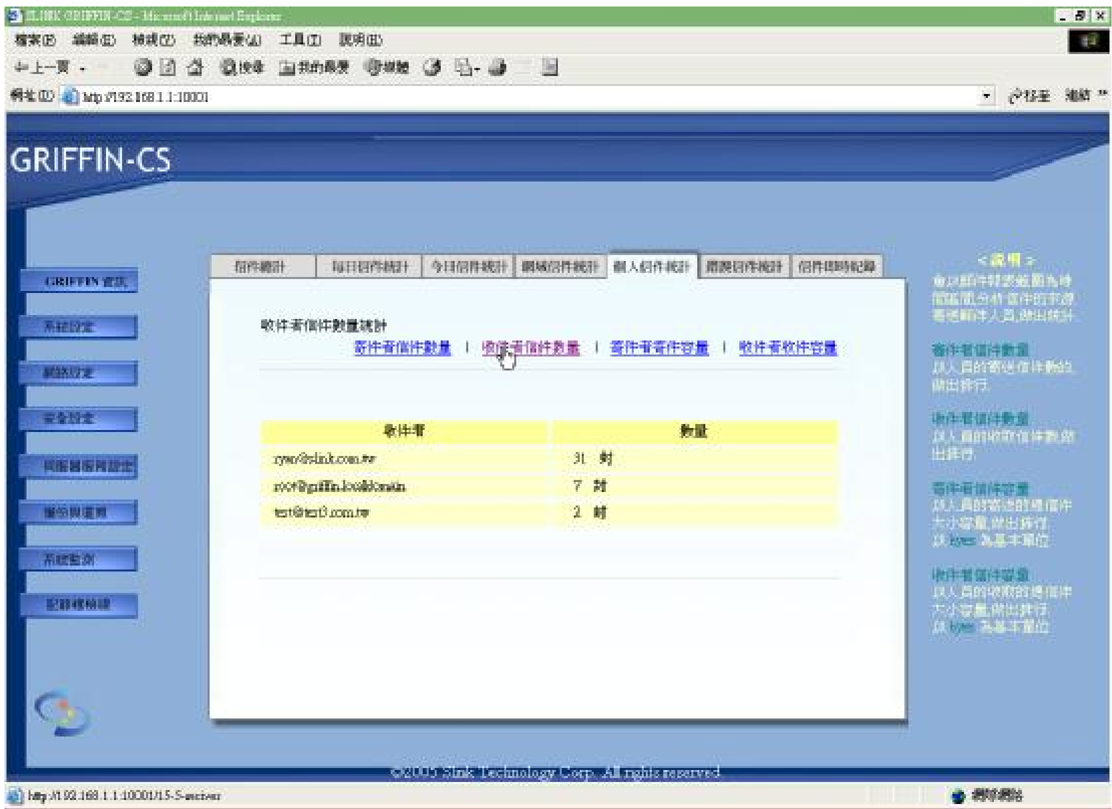
個人信件統計-寄件者信件數量統計

以使用者爲單位，統計出使用者寄件次數最多的排行



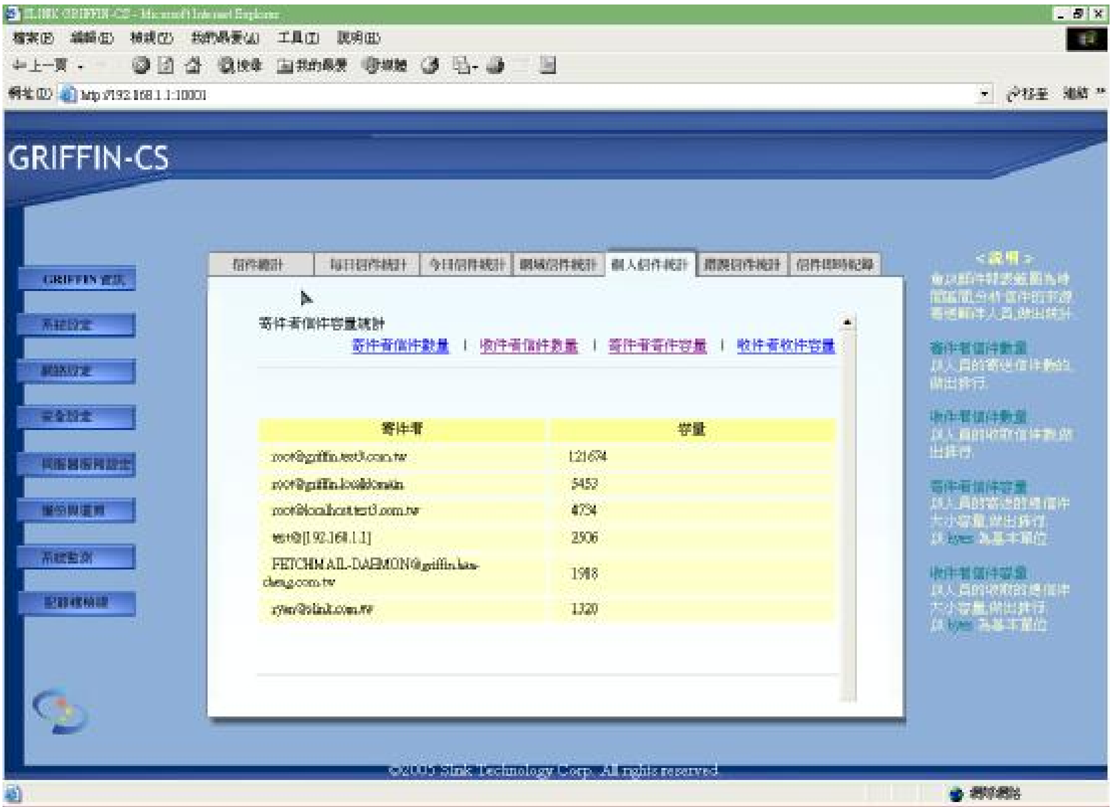
個人信件統計-收件者信件數量統計

以使用者爲單位，統計出使用者收件次數最多的排行



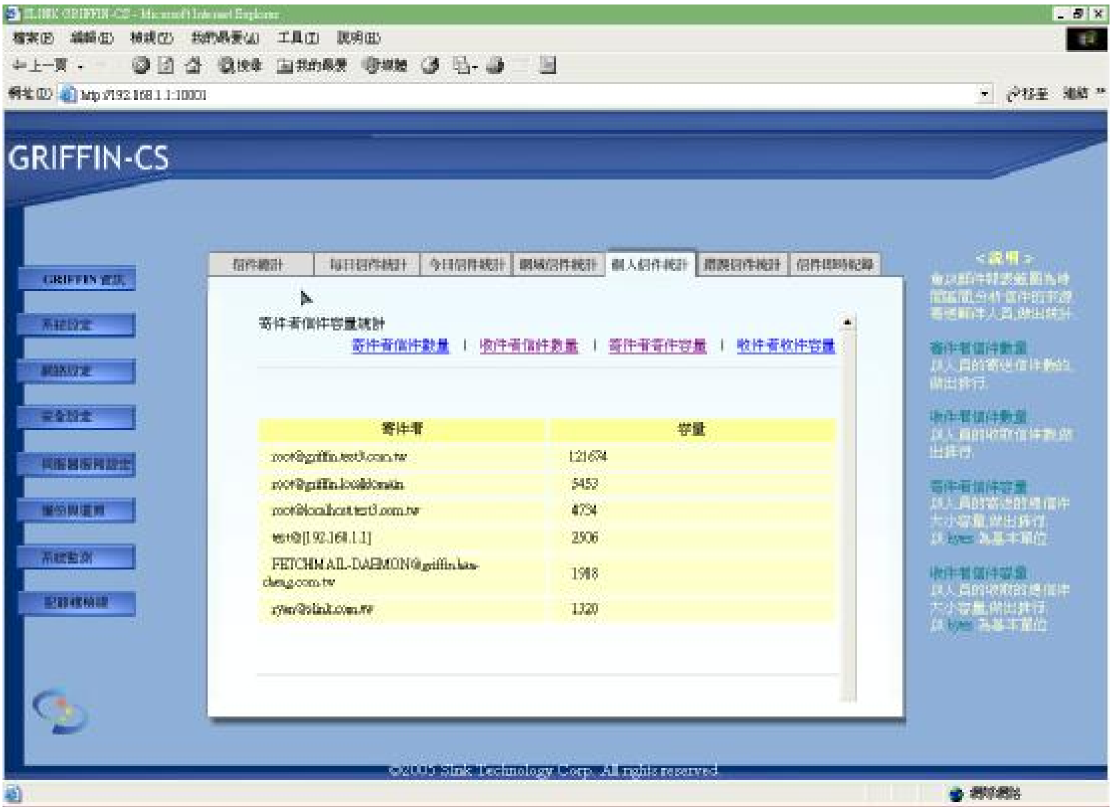
個人信件統計-寄件者信件容量統計

以使用者為單位，統計出使用者寄件容量（信件大小）最多的排行



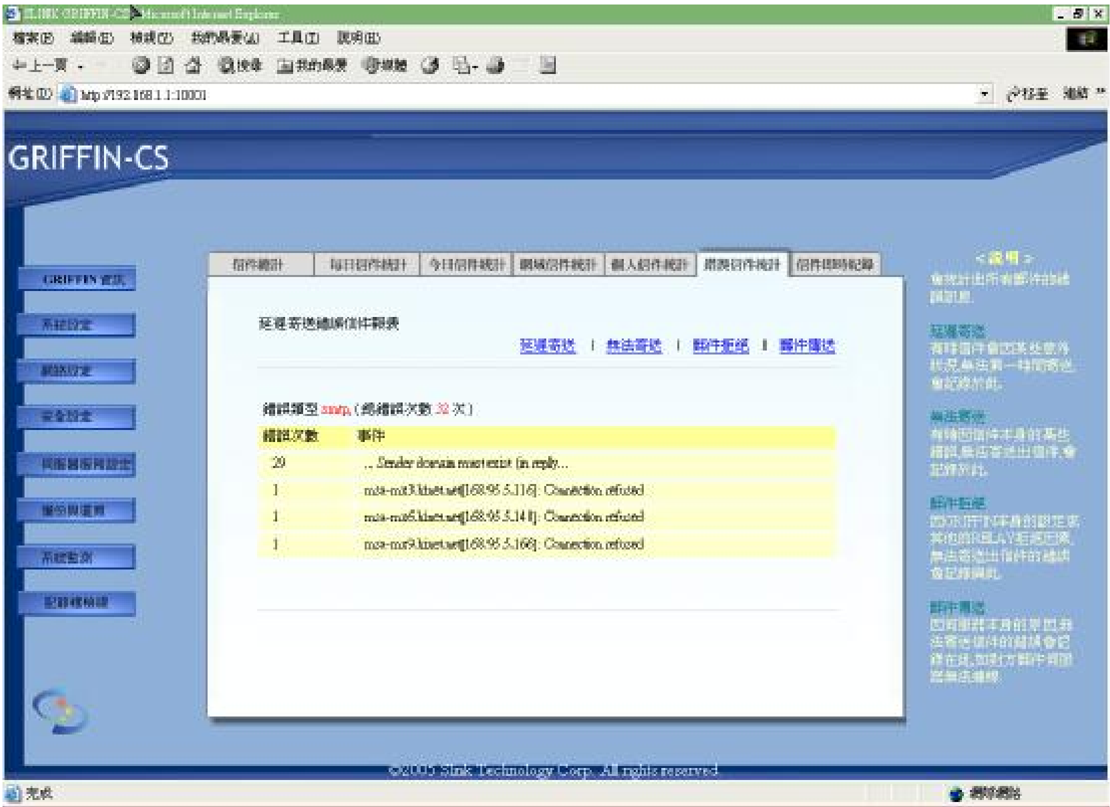
個人信件統計-收件者信件容量統計

以使用者為單位，統計出使用者收件容量（信件大小）最多的排行



錯誤信件統計-延遲寄送

統計所有信件發生延遲寄送的原因

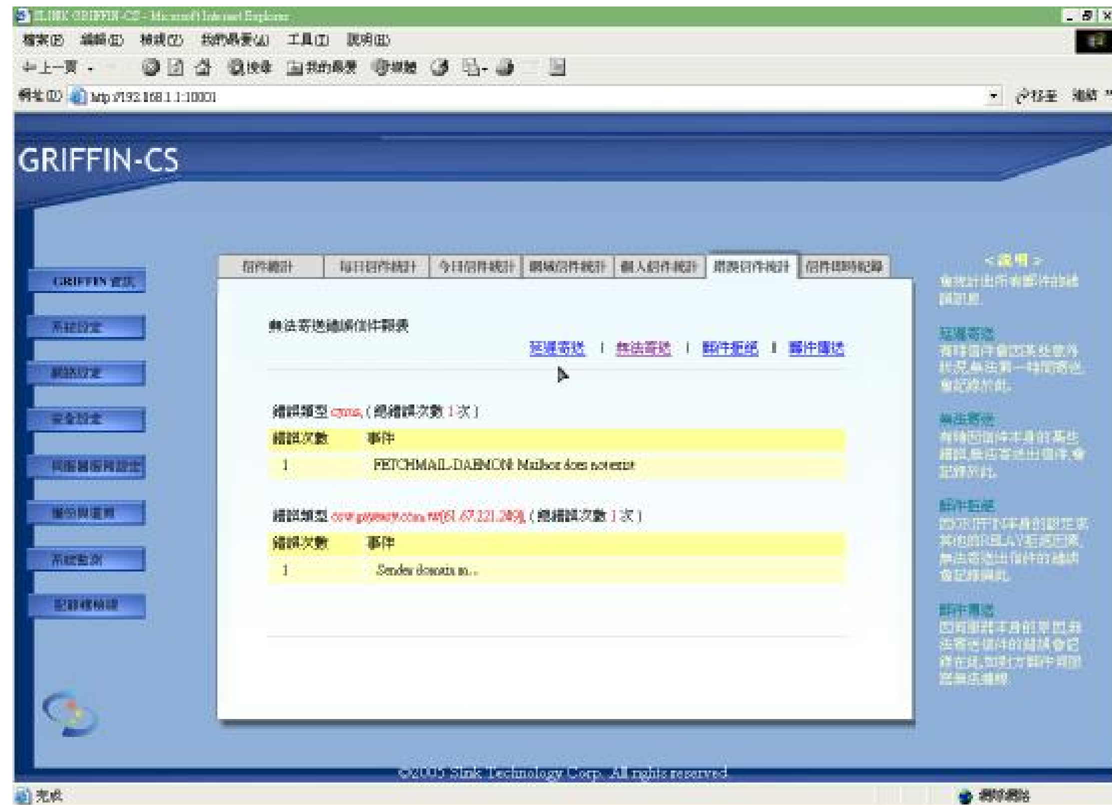


注意

信件延遲遲寄送不表示郵件由問題，而是可能是網路或一些其他因素的造成，信件的內容是無誤的。

錯誤信件統計-無法寄送

統計出信件無法寄送的原因記錄

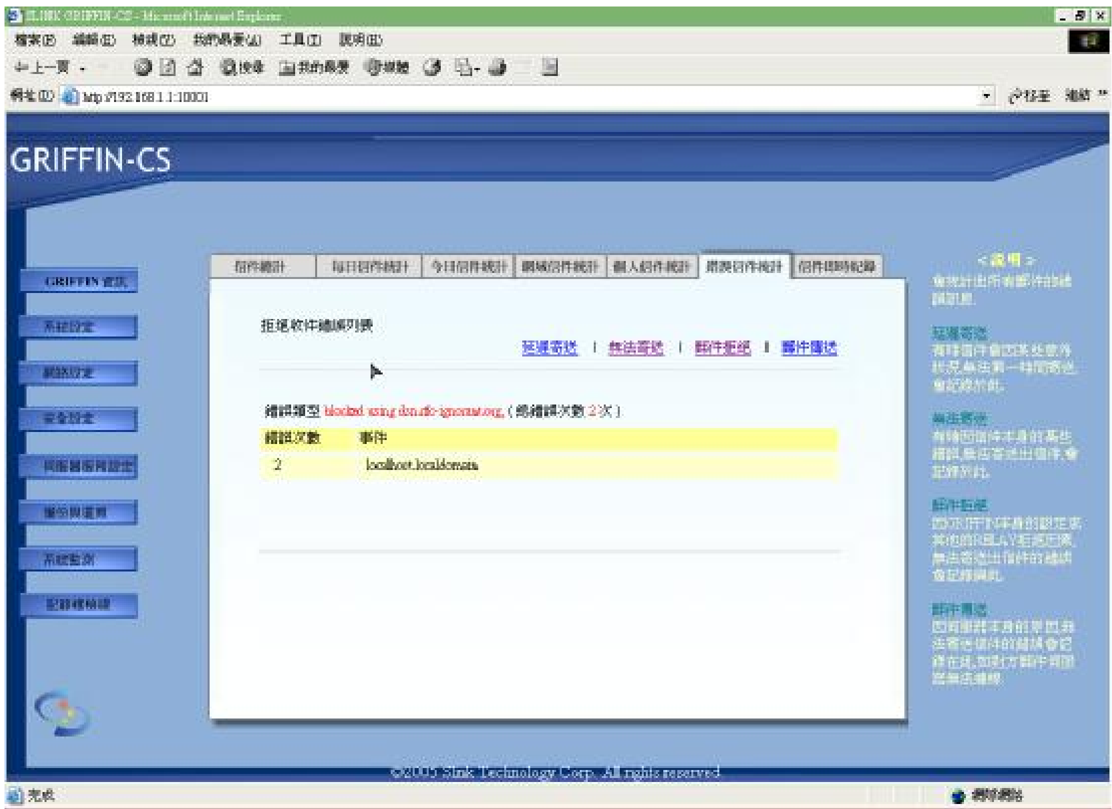


注意

信件無法寄送的原因有很多，如對方帳號不存在，信件超過伺服器允許大小、伺服器 RELAY 拒絕等，皆會記錄爲無法寄送錯誤。

錯誤信件統計-郵件拒絕

統計 GRIFFIN-CS2 拒絕郵件的原因次數

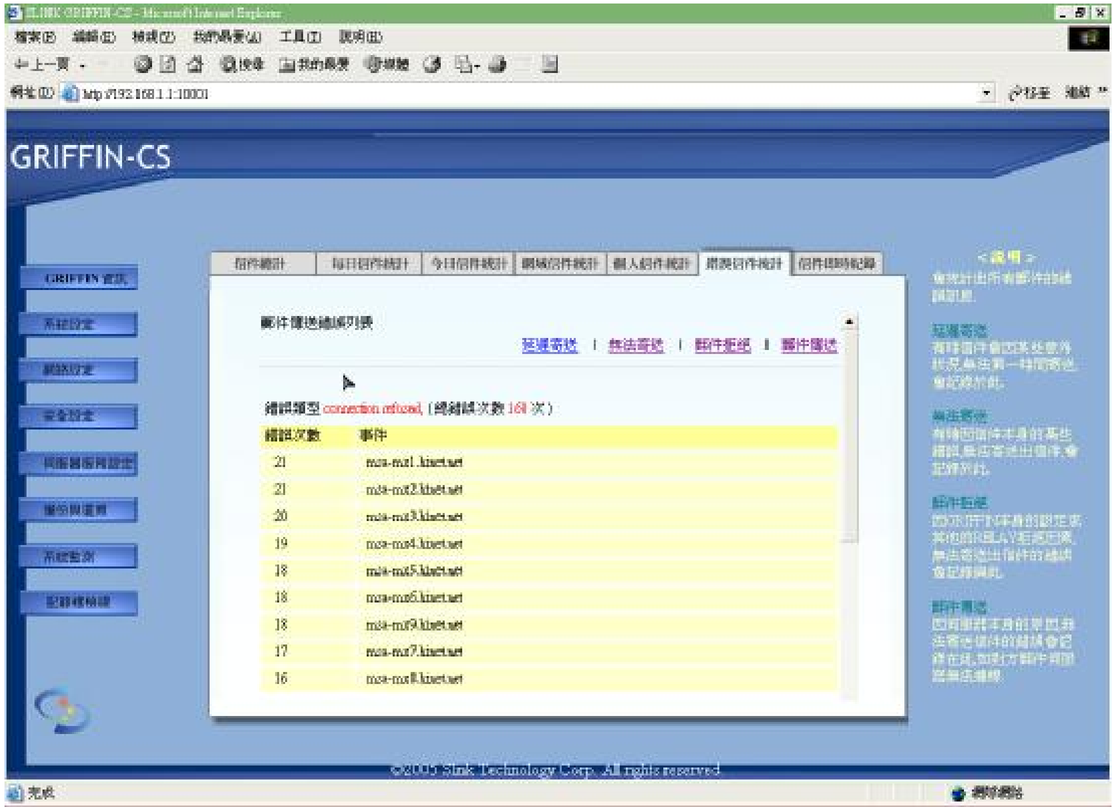


注意

GRIFFIN-CS2 拒絕收信的原因很多，如為 relay.org 的黑名單（如果由啓動此功能）、GRIFFIN-CS2 所設定的 RELAY 拒絕位置、不知名的內送使用者等。

錯誤信件統計-郵件傳送

統計所由因伺服器本身所發生的問題，造成的信件錯誤。

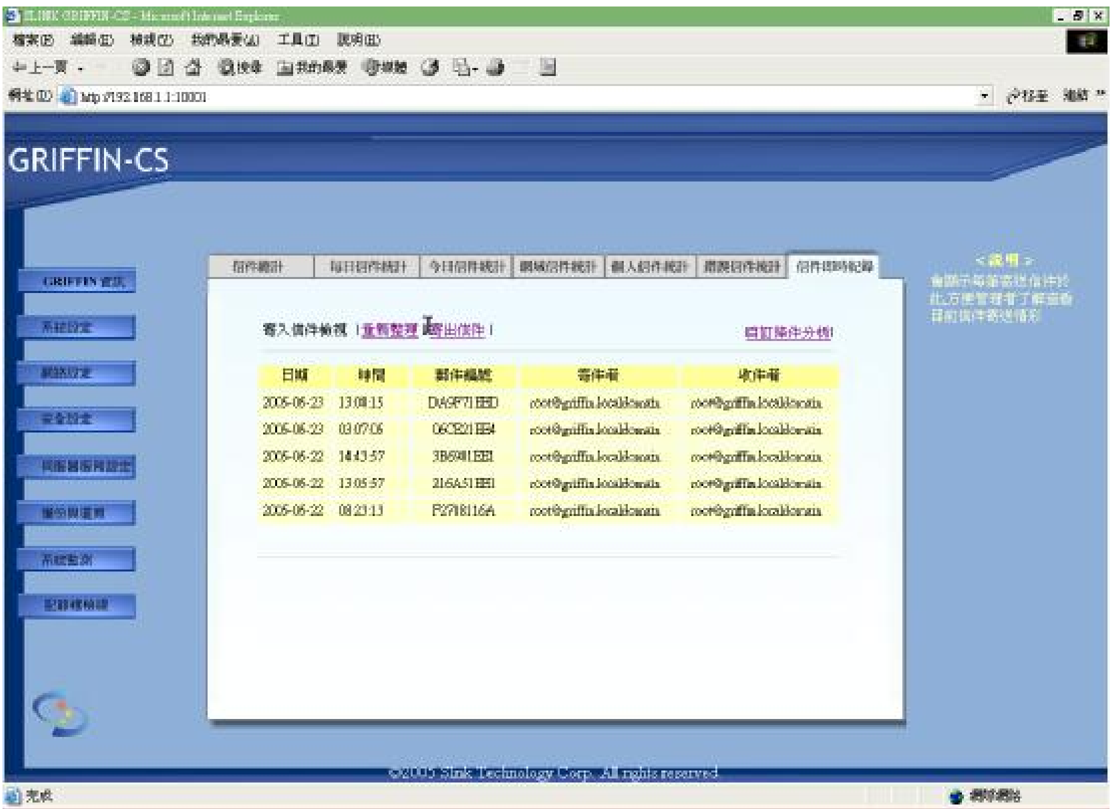


注意

如無法連接該伺服器、連線時間過長斷線、對方伺服器沒有提供郵件服務等，皆會被記錄爲郵件寄送錯誤

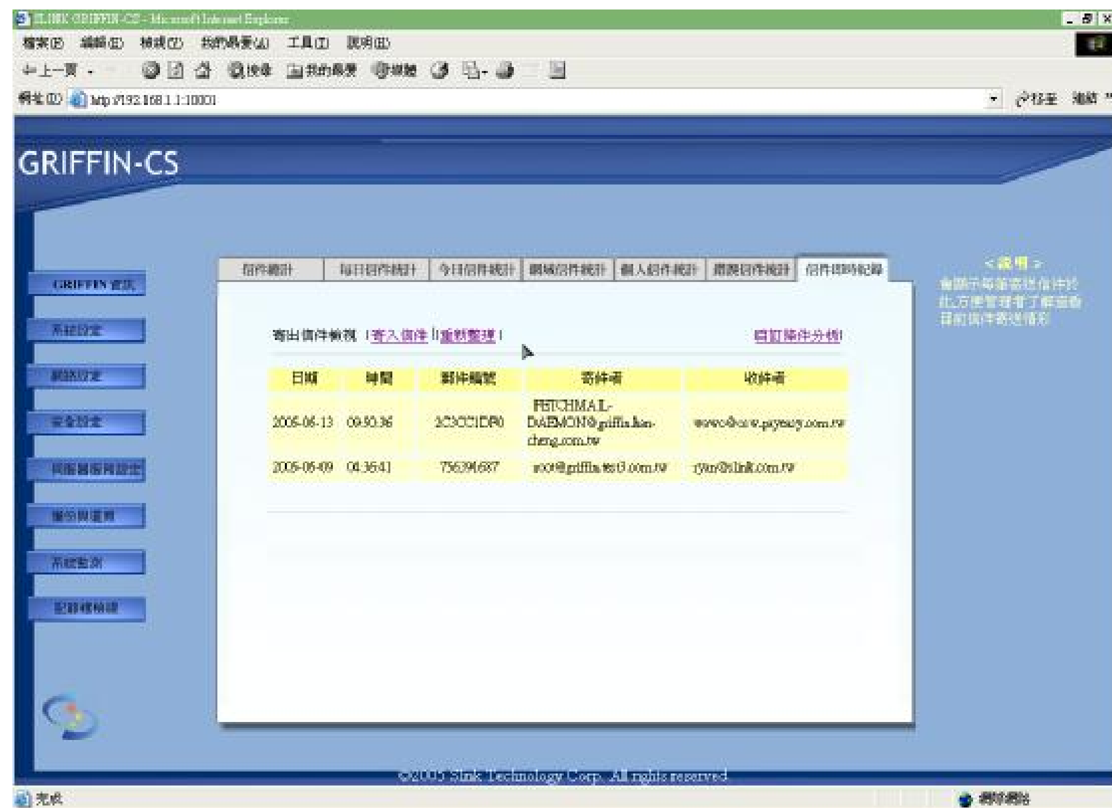
信件即時記錄-寄入信件檢視

信件即時記錄中的寄入信件檢視可以幫助管理者分析目前郵件伺服器收取的本機信件的處理狀態，何使用者寄信，收件者是誰，如果無法寄送，是何種錯誤造成，幫助管理者追蹤郵件的狀態。



信件即時記錄-寄出信件檢視

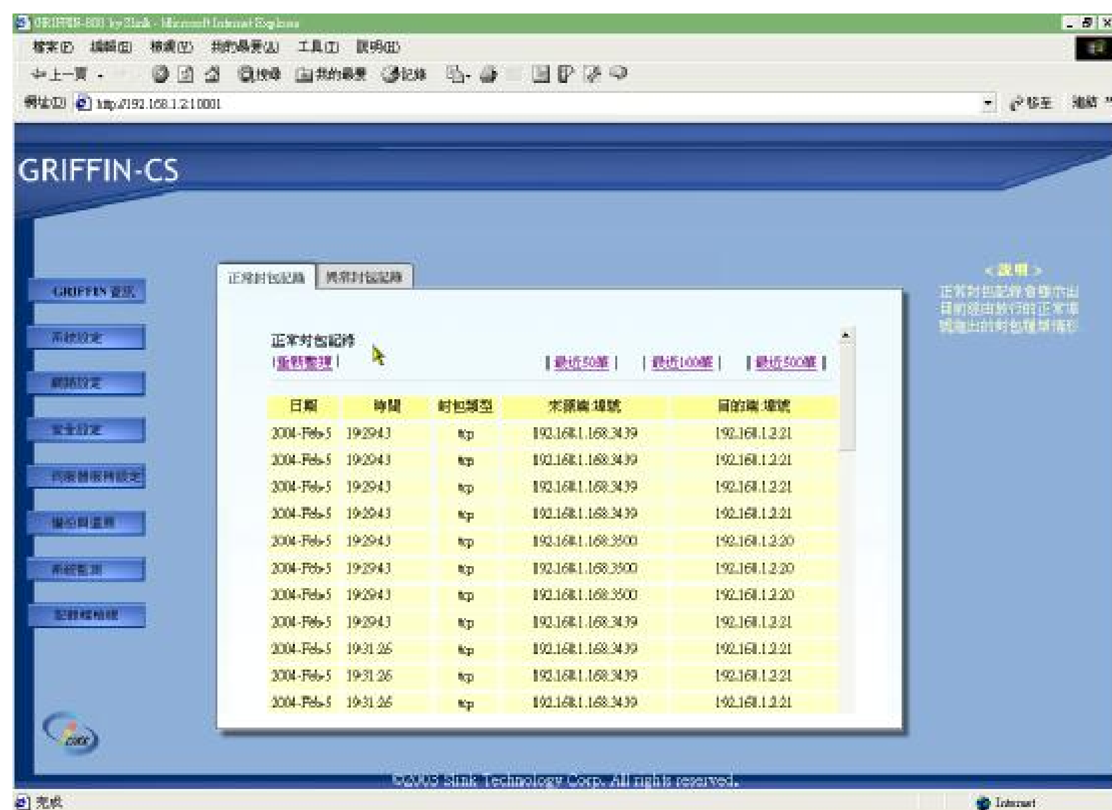
信件即時記錄中的寄出信件檢視可以幫助管理者分析目前郵件伺服器寄出的信件的處理狀態，何使用者寄信，收件者是誰，如果無法寄送，是何種錯誤造成，幫助管理者追蹤郵件的裝態。



防火牆記錄檔

正常封包記錄

當管理者在防火牆基本功能中有使用正常封包記錄時，所有的連線記錄便可以在這裡檢視



注意

本功能僅會分析最近一星期的資料

異常封包記錄

當管理者在防火牆基本功能中有使用異常封包記錄時，所有的不正常的連線記錄便可以在這裡檢視



注意

本功能僅會分析最近一星期的資料

客戶端密碼使用系統

GRIFFIN-CS2 目前提供客戶端密碼變更的客戶端功能，以減輕管理者的管理負擔，請各使用者開啓 Internet Explorer，鍵入

http://192.168.1.1:8585/

輸入管理者：umaster
管理者密碼：umaster（預設）

即會出現 GRIFFIN-CS2 使用者密碼變更系統畫面



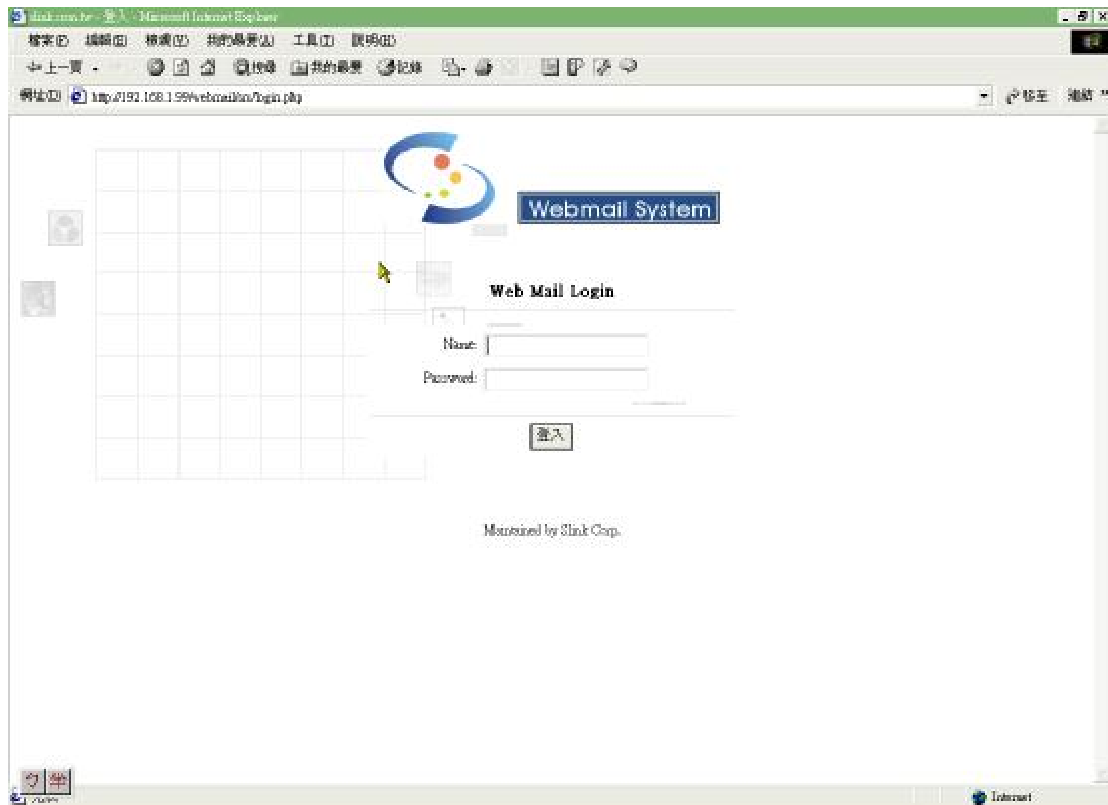
各使用者可以自行於此變更個人的密碼，而不需要再透過管理者。

此密碼爲各使用者的郵件帳號密碼，假設公司有啓用 SAMBA 功能，則此密碼亦爲登入 GRIFFIN-CS2 網路芳鄰目錄的密碼。

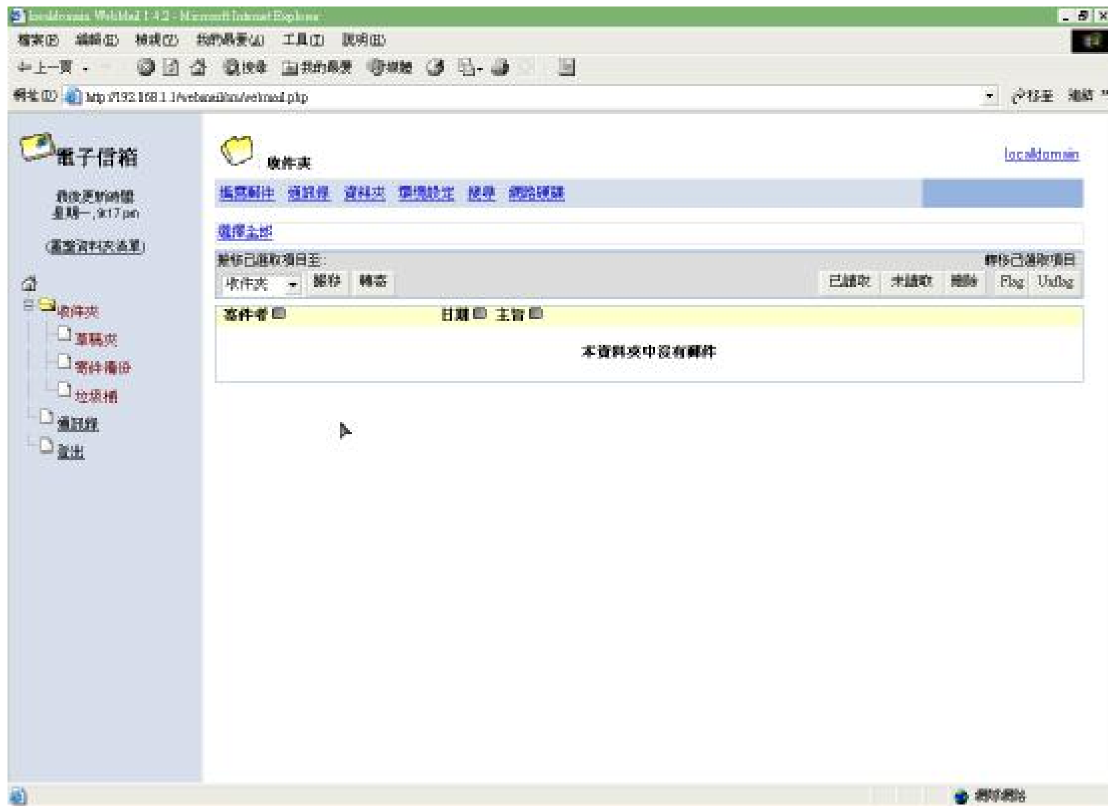
網路郵件系統的使用

當在網頁基本設定時，有使用 WEB MAIL 或網路硬碟時，重新啓動網頁伺服器後，鍵入 http://192.168.1.1/webmail/ （注意 webmail 後需加/）

便會出現 WEBMAIL 的首頁



使用者可以自行登入使用其功能，當有啓動網路硬碟時，便會出現網路硬碟選項，其上傳檔案的最大限制可以在伺服器設定/WEB 設定/基本設定中設定



使用者可以利用這系統去個人信件及放置個人檔案置網路上。

網路資訊簡易記錄表

閘道型架構

外部網路位置	位置 ____.____.____.____ 子網路遮罩 ____.____.____.____
內部網路位置	位置 ____.____.____.____ 子網路遮罩 ____.____.____.____
網路閘道	____.____.____.____
第一 DNS	____.____.____.____
第二 DNS2	____.____.____.____
管理者密碼	

內部單一網路架構

內部網路位置 1 （原本外部網路位置）	位置 ____.____.____.____ 子網路遮罩 ____.____.____.____
內部網路位置 2 （請設定爲不同網路區段）	位置 ____.____.____.____ 子網路遮罩 ____.____.____.____
網路閘道	____.____.____.____
第一 DNS	____.____.____.____
第二 DNS2	____.____.____.____
管理者密碼	

虛擬網路位置架構（需要 2 片 INTEL SERVER 等級網路卡）

外部網路位置	位置 ____.____.____.____ 子網路遮罩 ____.____.____.____
虛擬網路模式	□AFT □SFT □ALB □802.3ad
網路閘道	____.____.____.____
第一 DNS	____.____.____.____
第二 DNS2	____.____.____.____
管理者密碼	

相當感謝企業選擇思凌科技的 GRIFFIN-CS2 網路服務裝置爲您企業的網路服務建制方案，如果有任何 GRIFFIN-CS2 方面的技術問題，需要思凌科技爲您解決，則請

直接來電

886-7-5548258

886-7-5539166

或直接電子信箱

service@slink.com.tw

最後再次感謝您選擇本公司產品，希望能幫助貴企業踏出 E 化的第一步。

謝謝貴企業的選購